CyberGold

A Fully Automated and Common Good Monetary System

Christophe Lebrun, Arnaud Gaudinat, Ilan Leroux, Max-Florian Leroux,
Oetske Leroux-Fankhauser & Sébastien Leroux
{firstname-letter}.{lastname}@cifero.io (e.g. c.lebrun@cifero.io)

Version : v0.2

Abstract:

The CyberGold protocol, envisioned and orchestrated by the non-profit association Cifero, heralds a transformative phase in the stablecoin sector. As the digital economy evolves, stablecoins, which promise stability in the volatile world of cryptocurrencies, have gained paramount importance. Yet, many existing solutions grapple with challenges like governance risks, seigniorage revenue capture, and the trilemma of achieving decentralization, price stability, and capital efficiency concurrently.

Deep-rooted in the Cypherpunk ethos and inspired by the belief that monetary systems should unequivocally serve the public good, CyberGold emerges as a bastion of decentralization. The protocol is distinctly governance-free, guaranteeing both immutability and resistance to censorship. Its permissionless nature ensures universal access, reflecting a commitment to inclusivity. Central to its ethos is its peg to gold—a time-tested, decentralized asset. While CyberGold adeptly integrates with select third-party protocols for enhanced functionality, its foundational commitment to decentralization remains unwavering, always prioritizing system resilience and trust.

At its heart, the protocol champions a dual-role architecture, distinguishing between Stablecoin Users and Protocol Insurers. Stablecoin Users seek stability, providing par value at the point of purchase. In contrast, Protocol Insurers, bearing the market risks, fortify the protocol's reserves, acting as counterweights against market fluctuations. This division not only ensures CyberGold's unwavering peg but also sidesteps inefficiencies seen with overcollateralized Collateral Debt Positions (CDPs).

It's this very architecture, combined with full backing by a crypto-asset (Ether), that guarantees the much-vaunted "fully convertible" property, allowing users to directly swap CyberGold stablecoins and Ether, mirroring traditional currency exchanges. This system ensures a tangible stability anchor while optimizing asset utilization, and a responsive supply mechanism that adjusts to market demands.

An additional innovation lies in CyberGold's utilization of liquid staking, allowing the primary backing asset, Ether, to engage within a proof-of-stake mechanism. While this presents yield generation opportunities funneled to incentivize the protocol insurers, the protocol also astutely addresses the challenges of reserve liquidity risk associated with staking.

In essence, CyberGold marries the time-tested values of gold with cutting-edge technological advancements. As a fully decentralized protocol, where seigniorage revenues are equitably distributed among the protocol insurers who bear the risks, CyberGold offers unparalleled stability, complete convertibility, and optimized capital efficiency. Its architecture ensures absolute liquidity and a supply mechanism attuned to demand. In a world that seeks trust and efficiency, CyberGold sets a new gold standard for a digital currency tailored for our modern age.

Introduction

This White Paper offers a comprehensive understanding of the CyberGold protocol, its foundational philosophy, operational mechanics, and potential applications. Created by the not-for-profit association, Cifero[1], CyberGold emerges as a solution to the prevalent challenges in the existing stablecoin ecosystem.

A. Problem Statement

The Vital Importance of Stability in the Digital Economy

As the digital economy burgeons, the need for a reliable medium of exchange intensifies. Cryptocurrencies, with Bitcoin[2] as a prime example, carry the potential to revolutionize finance. However, their inherent volatility prevents them from optimally performing the three cardinal functions of money: acting as a medium of exchange, a unit of account, and a store of value. This unpredictability has catalyzed the ascent of stablecoins — digital assets meticulously designed to uphold a stable value, typically anchored to national currencies like the U.S. Dollar.

Stakes of Decentralization in Stablecoins

Despite their growing importance and utility, from enabling DeFi operations to streamlining international remittances and routine transactions, stablecoins are encumbered with several challenges:

- **Reliance on Fiat Currencies:** Many stablecoins, by pegging their value to fiat currencies, inadvertently tether their fate to the central banks monetary policies. If the fiat currency undergoes inflation, devaluation, or any form of economic tumult, the stablecoin's credibility is immediately jeopardized, defying the core principles of decentralization embodied by cryptocurrencies.
- **Governance Risks:** Stablecoins are frequently ensnared in governance quandaries. Centralized governance is a magnet for manipulations, external interventions, and regulatory headwinds. Conversely, while Decentralized Autonomous Organizations (DAOs) diminish central control points, they remain vulnerable to collusion and dominant influences, sometimes jeopardizing their core democratic ethos.
- **Seigniorage Revenue Captation:** Seigniorage, or the revenue from issuing new coins, often benefits specific entities or factions, especially within decentralized structures like DAOs. This revenue-driven stance can, at times, foster misaligned

[1] CIFERO

[2] *Bitcoin: A Peer-to-Peer Electronic Cash System*, Satoshi Nakamoto

priorities, jeopardizing the broader stability or trustworthiness of the stablecoin mechanism.

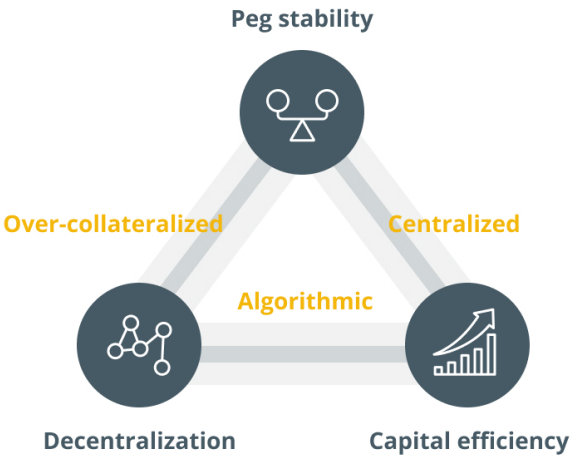
Other Crucial Dimensions for a Holistic Stablecoin

Emerging trends underscore additional attributes pivotal for a comprehensive stablecoin solution:

- **Convertibility:** Ensuring seamless conversion between the stablecoin and other assets with minimal impediments.
- **Solvency:** Continuously guaranteeing ample reserves or assets to back the stablecoin.
- **Market Liquidity:** Ensuring the stablecoin can be swiftly traded without inducing drastic price shifts.
- **Reserve Liquidity:** A protocol's prowess in preserving a cache of liquid assets, crucial for honoring conversion requests. For stablecoins, this ensures that holders can invariably redeem their assets at the pegged rate, even amidst market volatility.
- **Capital Efficiency**: Refers to the optimal use of capital within the protocol. An efficient system minimizes idle capital, ensuring productive use of assets.

The Landscape of Stablecoins and the Trilemma Challenge

The realm of stablecoins is filled with inherent trade-offs, among which the Stablecoin Trilemma[3] is one of the most debated. This trilemma asserts that it's notably challenging to achieve three core attributes simultaneously: decentralization, price stability, and capital efficiency.



The stablecoin trilemma (source: cointelegraph.com)

[3] *Le trilemme du stablecoin*, Martin Vernay

Stablecoins can typically be categorized into three main archetypes based on their operational mechanism:

1. **Centralized Fiat-Backed Stablecoins**: USDC and Tether (USDT) are prominent examples that peg their value to fiat currencies. While they excel in delivering price stability and capital efficiency, their dependence on centralized entities for reserve management raises concerns about transparency, trust, and potential regulatory interference.
2. **Algorithmic Stablecoins**: These rely on algorithms and smart contracts to adjust the coin's supply, aiming to maintain its peg, often to a fiat currency. While they prioritize decentralization and sometimes even capital efficiency, their consistent challenge remains in maintaining price stability, especially during volatile market conditions.
3. **Overcollateralized Crypto-backed Stablecoins**: Platforms like MakerDAO's DAI[4] are archetypes of this category. They use cryptocurrency assets, exceeding the stablecoin's face value, as collateral. These coins effectively meld decentralization with price stability but often compromise on capital efficiency, as a significant portion of the capital remains dormant to maintain their peg.

Navigating these intricate dimensions and striking an optimal equilibrium without compromises remains a formidable challenge. This is where innovative solutions like CyberGold enter the narrative. As a progressive protocol, CyberGold is not just another player in the game but aspires to be a game-changer, meticulously designed to address these nuances and present a holistic solution for the next era of stablecoins. In the subsequent sections, we'll delve deeper into how CyberGold seeks to redefine the stablecoin paradigm.

B. Solution: CyberGold Protocol

Introducing the CyberGold protocol, this section sheds light on how it harnesses blockchain technology combined with a gold peg, aiming to deliver a stablecoin that is transparent, decentralized, and reliable. Born from the initiatives of Cifero, a non-profit association, CyberGold operates as an ERC-20[5] compliant token with the robust backing of independent crypto-assets, ensuring its users the promise of high stability and full convertibility.

Concept and Design

The CyberGold stablecoin is deeply rooted in the ethos of the cypherpunk movement. Emerging prominently in the late 20th century, the cypherpunk movement championed

[4] MakerDAO
[5] ERC-20 Token Standard | ethereum.org

cryptography as a tool to ensure personal privacy and freedom against centralized forces. Reflecting these principles, CyberGold emphasizes decentralization, immutability, and transparency—core values that resonate with the wider aspirations of the crypto community.

At the heart of CyberGold's ethos is its unwavering commitment to the non-profit principle. Cifero, the association spearheading CyberGold's development, is deeply rooted in a vision centered on the collective benefit. While it leads the developmental charge, the protocol itself remains devoid of governance, ensuring all operations are automated and free from human biases. This design, crafted for and by the community, prioritizes delivering a dependable and consistent digital asset, emphasizing the common good above all.

In further adherence to these principles, CyberGold is open-source. Once deployed, the contract stands immutable, free from proxy contracts or any privileges or profit for its developers, ensuring a truly permission-less experience.

Fully decentralized protocol

CyberGold stands as a beacon of decentralization in the modern financial landscape. Committed to the principles of immutability, openness, and a governance-free framework, it signals a move towards a financial system free from undue control and centralized influences.

A key facet of CyberGold’s design is its strategic anchoring to gold. Historically, gold has served not just as a symbol of affluence but as a decentralized asset, impervious to the whims of governments and central banks. By aligning its value with gold, CyberGold combines the steadfast reliability of this precious metal with the advantages of the digital realm.

Yet, CyberGold isn't simply a digital representation of gold. It's a digital asset underpinned by a public blockchain crypto-asset, Ether, ensuring both security and decentralization. This integration promises enhanced liquidity, boundless supply, superior divisibility, and the convenience inherent to digital assets.

In its essence, CyberGold seeks to bridge traditional value with the transformative capabilities of blockchain technology, emphasizing a system that looks out for the collective benefit of all its users.

Fully backed stablecoin

CyberGold distinguishes itself through a clear separation between its "tracked asset" and its "backing asset". While its value is pegged to gold, a globally recognized standard of value, it's primarily backed by a crypto-asset: Ether, the native coin of the Ethereum[6] ecosystem. By being backed by an exogenous asset, whose price isn't correlated with CyberGold token

[6] https://ethereum.org

value, CyberGold sidesteps the death spiral threat that plagues pure algorithmic stablecoins[7].

CyberGold differentiates itself not just from pure algorithmic stablecoins but also from overcollateralized crypto-backed stablecoins like DAI, by segregating stability seekers from stability providers. Therefore, the CyberGold protocol presents two types of actors:

1. **Stablecoin Users:** These actors' primary aim is to seek stability in their holdings. They anchor CyberGold's immediate worth by providing the par value at the time of purchase.
2. **Protocol Insurers:** These actors play a crucial role in the CyberGold ecosystem. Entrusted with bearing the market risk, they ensure that the protocol remains fully backed even amidst turbulent market shifts. Their commitment to fortifying the protocol's reserves, acting as a buffer against volatility, isn't without its rewards. Beyond the inherent benefits of a leveraged position, they partake in the protocol's revenue, creating a mutualistic relationship where both the protocol and the insurers thrive.

The symbiotic relationship between these two roles ensures CyberGold's peg without the inefficiencies commonly associated with overcollateralization. To handle the market fluctuations, a dedicated Rebalancing Mechanism comes into play. When the value of the backing asset decreases, reserves (primarily funded by protocol insurers) bolster the PrimaryPool, safeguarding the full backing of the CyberGold stablecoin[8]. Conversely, when the backing asset's value increases, the surplus is funneled into the reserves (*SecondaryPool*), creating benefits for the solvency insurers.

By marrying this dual-role architecture with the rebalancing strategy, CyberGold offers a distinct fusion of stability and efficiency.

Fully convertible stablecoin

The concept of full convertibility stands at the very core of CyberGold's design, setting the stage for a stablecoin experience unlike any other. Users are afforded the flexibility to directly purchase CyberGold stablecoins, exchanging their Ether for this novel asset, much like swapping between two distinct currencies. This transaction simplicity is crucial: they're not pledging Ether as collateral but are making a straightforward acquisition of CyberGold stablecoins at par-value.

However, the true advantage lies in the additional features this full convertibility brings to the table. It acts as the bedrock of CyberGold’s stability. By ensuring that users can, at any time, redeem their CyberGold for a portion of the PrimaryPool (which typically aligns with the par value), it provides a tangible anchor that closely ties the market price of CyberGold to the universally recognized value of gold. This dynamic doesn’t just promise stability; it actively enforces it, ensuring that even amidst market turbulence, CyberGold remains steadfast.

---

[7] *On the Economic Design of Stablecoins*, Christian Catalini and Alonso de Gortari
[8] Note: Such mechanism has been explored by stablecoins such as StatiCoin/RiskCoin, AngleProtocol, Djed/Shen, f(x) protocol.

Capital efficiency is another hallmark of this system. In many traditional setups, vast amounts of capital lie dormant or underutilized. CyberGold, with its emphasis on full convertibility, avoids such pitfalls. It assures that every unit of the stablecoin in circulation is matched, thereby optimizing the use of assets and creating an environment where financial resources are used to their fullest potential.

This efficiency seamlessly blends with the elastic supply mechanism. The full convertibility property ensures that CyberGold responds in real-time to the ebbs and flows of market demand. This adaptive nature means that the supply of CyberGold stablecoins is a reflection of the prevailing market sentiments, adjusting as needed.

However, as with any robust system, there are necessary checks in place. Small fees are levied on both the issuance and redemption operations. These fees serve a dual purpose. Firstly, they act as a safeguard against potential vulnerabilities, such as oracle front-running attacks. Secondly, they provide incentives for protocol insurers, ensuring the protocol's continued health and stability. It's essential to recognize that these fees introduce a spread — a term denoting the minor difference between the buying and selling price.

In weaving together these facets of full convertibility, CyberGold crafts a stablecoin narrative that is not only stable but also efficient, responsive, and secure.

Fully liquid protocol

Within the architecture of the CyberGold protocol, there's a noteworthy utilization of liquid staking. The primary backing crypto asset (Ether) is engaged within a liquid staking protocol. This engagement results in capital yield which, in turn, is channeled to encourage increased hedging by the protocol insurers.

Additionally, by involving the backing asset in the proof-of-stake mechanism, the protocol also contributes to the securitization of Ethereum, the underlying layer-1 blockchain. This function illustrates how CyberGold operates as a component within the broader blockchain ecosystem.

This method, while innovative, introduces the challenge of reserve liquidity risk. Due to the nature of staking, assets in the staking protocol might not be as immediately accessible compared to their non-staked counterparts. To address this, the protocol provides an option where users can redeem liquid staking tokens (LSTs), when facing liquidity constraints.

In integrating liquid staking with a systematic approach to liquidity management, CyberGold presents a comprehensive solution addressing both yield generation and liquidity challenges in the crypto domain.

C. Use cases

The inception of CyberGold brings forth a stablecoin that's not only decentralized but is also independent from traditional fiat systems. This enables distinctive applications, particularly in scenarios where immunity to governmental oversight and censorship is crucial.

1. **Censorship-Resistant Transactions:** In regions where the government exerts strict control over financial transactions, CyberGold offers a decentralized alternative. Being pegged to gold and not to any fiat currency, it can bypass governmental restrictions, enabling free trade and financial interactions.
2. **International Remittances:** CyberGold facilitates seamless cross-border payments, making it especially valuable for countries with limited access to international banking avenues. With CyberGold, residents have the means to send and receive funds on a global scale without the dependence on traditional banking channels.
3. **Wealth Preservation in Economically Volatile Regions:** For residents of countries facing economic instability, hyperinflation, or political turmoil, CyberGold provides a way to store value securely without relying on the local fiat currency. This ensures their wealth is insulated from domestic economic upheavals.
4. **Decentralized Autonomous Organizations (DAOs):** DAOs, by design, operate independently of any central authority. Using CyberGold as a treasury asset or means of transaction within the DAO ecosystem ensures complete decentralization, aligning with the core principles of DAOs.
5. **Global Crowdfunding and Fundraising:** For initiatives that address global challenges or are of international relevance, fundraising needs to be independent of any specific nation's fiat system. CyberGold can be the medium for such global fundraising efforts, ensuring contributions are transparent, decentralized, and free from governmental interference.
6. **International Trade and Commerce:** For businesses operating across borders, especially in regions with strict trade regulations or unstable fiat currencies, CyberGold can serve as a universal medium of exchange. It facilitates trade agreements without the hurdles of currency conversions or governmental red tape.
7. **Gaming and Multiverse Economy:** CyberGold's decentralized nature positions it as an ideal currency for online gaming and multiverse economies. It ensures true ownership of in-game monetary assets and its interoperability facilitates seamless cross-game monetary asset transfers between interconnected virtual worlds.

Key Takeaways

Pioneering Stablecoin Vision: The CyberGold protocol, orchestrated by the non-profit association Cifero, signals a seminal moment in the stablecoin sector. By marrying blockchain's transparent and decentralized capabilities with gold's unwavering stability, CyberGold emerges as a formidable contender against the inherent frailties of current stablecoin solutions, suffering from centralization, inadequate backing, illiquidity or capital inefficiency.

Design Blueprint: CyberGold meticulously sidesteps these pitfalls. It offers an evolved blueprint that not only fortifies decentralization but also ensures full convertibility with its overarching positive consequences in terms of stability, capital efficiency and responsive supply.

Versatile Applications: Crafted to cater to a wide range of requirements, from individuals in unstable economic landscapes to multinational businesses, the protocol offers solutions that are both broad in scope and specific in application. From underpinning censorship-resistant transactions to steering the financial mechanics of expansive virtual universes, CyberGold positions itself as a linchpin of innovation. It represents a financial model that seamlessly bridges time-honored monetary principles with avant-garde technological breakthroughs, thus ushering in an era of transparent, dependable, and holistic financial interactions.

As we progress to the following chapters, readers are invited to a comprehensive dissection of CyberGold, demystifying each intricate mechanism that fuels this pioneering protocol.

1. Fully decentralized protocol

In the introduction, we unveiled the foundational principles behind CyberGold – a novel fusion of age-old trust in gold and groundbreaking blockchain technology. As we venture further, it's essential to understand what truly sets CyberGold apart in the crowded financial landscape: its unwavering commitment to decentralization.

Decentralization isn't just a buzzword for CyberGold; it's the lifeblood that runs through every aspect of its design and functionality. This chapter will guide you through the facets of CyberGold's decentralization, from its immutable and censorship-resistant nature to its leveraged third-party protocols. By the end, you'll have a clear grasp of how CyberGold is pioneering a financial revolution, staying true to the decentralized essence of blockchain, and carrying forward the timeless value of gold into the digital realm.

1.1. Immutability and censorship resistance

The blockchain realm is filled with promises of immutability, but CyberGold takes this principle to the next frontier, ensuring unchanging stability and unwavering trust. While many blockchain projects might use the term "immutable" to describe their protocols, nuances exist in their practical application of this principle. On platforms like Ethereum, while the transactional records and smart contract codes are immutable, several protocols retain mechanisms allowing for adjustments to their operational dynamics post-deployment.

CyberGold, in stark contrast, champions a future-proof approach. Once its smart contract is deployed on the Ethereum platform, the protocol operations are eternally fixed. This is not just about the code being unchangeable; it's about the protocol's very essence, its functionality, and its principles remaining steadfast through time.

There are no mechanisms like proxy contracts to sidestep this rigidity by redirecting or upgrading the core protocol without users control. No constant value within the protocol can be altered. Fundamentally, it's devoid of any governance mechanism. This ensures that the protocol, post-deployment, is free from any form of change – whether in response to market dynamics, community pressures, or any other external factors. Such a design ethos translates to unparalleled trust. Users can rest assured that the CyberGold they interact with today will operate under the same principles tomorrow, the next year, and beyond.

Now, deriving from this profound immutability is the concept of censorship resistance. It's not just that no single entity can alter or obstruct the CyberGold protocol; the reality is even more profound. No entity at all, including its creators, has the power to stop or modify its operation. The only conceivable way to interrupt CyberGold would be to halt the entirety of the Ethereum network itself—a testament to the robustness of its design.

In an era riddled with uncertainties, be it in the technological or financial spheres, CyberGold provides a bedrock of stability. It assures its users of a consistent, unchanging experience, not just by virtue of code immutability but by ensuring its core functionality remains unaltered. In doing so, it epitomizes the very essence of trust in the decentralized world.

1.2. Permissionless Nature and Trustlessness

In a landscape dominated by ever-evolving financial technologies, the concepts of "Permissionless" and "Trustless" emerge as guiding principles for decentralized platforms like CyberGold. These principles reinforce CyberGold's commitment to an inclusive and transparent ecosystem.

Permissionless: Being "permissionless" encapsulates the essence of unrestricted access. Regardless of one's location, identity, or economic background, everyone can engage with the CyberGold protocol. This unrestricted approach allows for a more democratized interaction where all users can fully experience the benefits of the protocol without artificial barriers.

Trustless: The term "trustless" might be slightly misleading upon first glance. It doesn't denote an absence of trust, but rather a redirection of it. Instead of relying on third-party entities, CyberGold places trust in transparent algorithms, mathematics, and the immutable nature of its protocol. This mechanism ensures users can engage confidently, knowing that their interactions are backed by robust and transparent system mechanics. Security in such a trustless environment is inherently amplified. Without the necessity for intermediaries, the system minimizes potential vulnerabilities and attack vectors, lending itself to robust resilience.

The advantages of decentralization as exhibited by CyberGold are manifold. With the removal of traditional hierarchies and restrictions, every participant enjoys an equitable stake and an unfiltered voice in the ecosystem. The approach underscores a financial system that’s designed with inclusivity and transparency at its heart.

In essence, CyberGold isn't just another digital currency. It embodies the very essence of decentralized finance: it's open, inclusive, and empowering. Above all, it ushers in a fair ecosystem that aligns seamlessly with the broader financial world.

1.3. Money as a Common Good

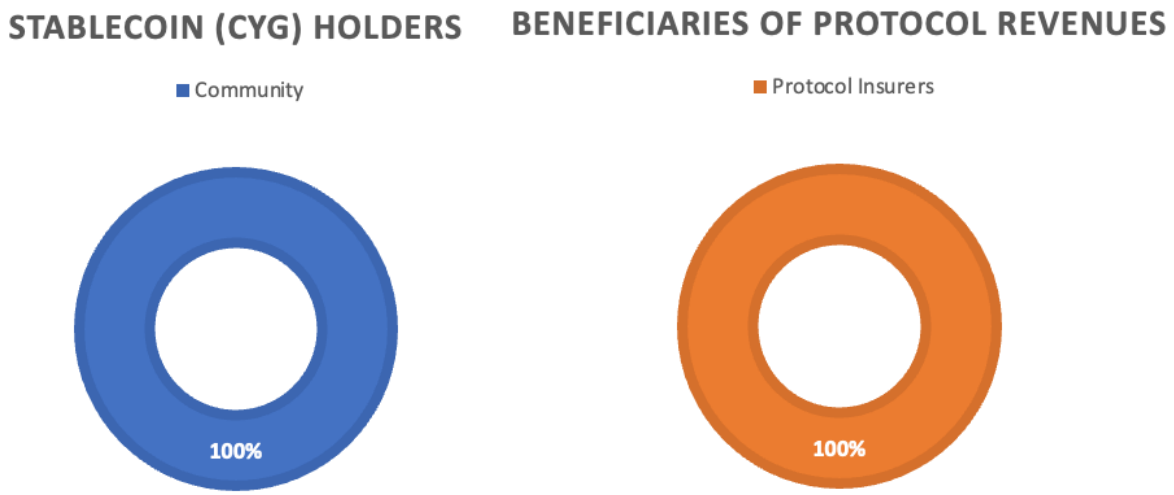
Historically, the concept of money has evolved significantly. From barter systems to gold coins, and from paper currencies to digital assets, the form and function of money have shifted to suit the demands of society. At its core, though, the primary role of money remains unchanged: it acts as a medium of exchange, a unit of account, and most importantly, a store of value.

However, as economies grew complex, the very essence of money began to be influenced by a host of external factors - geopolitical tensions, economic policies, centralized control, and even speculative trading. These influences have sometimes caused money to deviate from its primary purpose, particularly when its stability is jeopardized.

Moreover, in various systems, the seigniorage revenues - the profits made by issuing currency - are extorted from its users and illegitimately land in the coffers of issuers. This includes national governments, private banking institutions or even protocol stakeholders in

allegedly decentralized ecosystems. This pattern deviates from the ideal of money as a community asset truly belonging to its users.

CyberGold heralds a new approach in the stablecoin ecosystem. Conceived as a communal asset, it's a stablecoin crafted by the community, for the community. Unlike many modern crypto systems, CyberGold doesn't distribute governance tokens granting special privileges, whether financial or otherwise, to its development team or early investors. Instead, its protocol revenues, reminiscent of seigniorage revenues, are directed as insurance premiums. These premiums serve as compensation for the protocol insurers, who stand at the frontline, poised to reap profits when the protocol thrives, yet equally prepared to shoulder losses when challenges arise. In essence, CyberGold ensures that the financial gains from its operation directly bolster its resilience and stability. It stands as a testament to a monetary system where rewards are aligned with tangible contributions, preserving the ethos that a community-driven financial system should be equitable and all-encompassing.



1.4. Gold - The Ultimate Decentralized Asset

The tale of human civilization is, in many ways, intertwined with the story of gold. From ancient Egyptian pharaohs to modern-day central banks, gold has played a pivotal role as a symbol of wealth, power, and stability. Throughout history, civilizations have adopted gold as a universal currency, not merely for its lustrous appeal but for its intrinsic value and enduring nature.

Gold stands out as an asset that transcends borders and epochs. Unlike fiat currencies, which are subject to inflationary pressures, political decisions, and economic policies, gold has largely maintained its purchasing power over long stretches of time. This preservation of value stems from its scarcity, non-corrosiveness, and the fact that its worth isn't dictated by governmental decrees or policies. In this light, gold is truly decentralized, making it a natural choice to back a currency aspiring for the same ideals.

Choosing gold as the anchor for CyberGold isn't just a nod to history or a preference for shiny metal; it's a conscious alignment with the protocol's foundational principles. The

cypherpunk movement, from which decentralized systems draw much inspiration, emphasizes freedom from central controls and undue interference. Gold, with its inherent resistance to centralized manipulation, perfectly embodies this ethos.

Furthermore, for the sake of practicality and usability in modern economic contexts, CyberGold is pegged to the price of one tenth of a gram (or 100mg) of gold. This peg ensures that while CyberGold inherits the stability and reliability of gold, it also becomes sufficiently divisible, making it suitable for everyday transactions and as a unit of account in digital financial systems.

1.5. CyberGold - advantages of a digital asset

Physical gold, for all its glittering allure and enduring value, comes with its set of challenges. Storage requires secure facilities, often at a significant cost. Transportation across borders can be cumbersome, and the process is fraught with logistical hurdles. Moreover, transacting in gold, especially in small amounts, is far from practical in a world where speed and convenience are paramount.

CyberGold encapsulates the stability of gold while supercharging it with the myriad benefits of a digital asset : liquidity, unlimited supply, divisibility, full custody, trustless operations, transactional speed, cost-efficiency, non-custodial nature, and borderless capabilities.

In essence, CyberGold is not merely a digital representation of gold; it's an enhancement. By merging the timeless value of gold with the innovative advantages of the digital age, CyberGold presents a solution tailored for the contemporary world, making it an attractive choice for those yearning for stability in the dynamic crypto environment.

1.6. Leveraging third party decentralized protocols

In the decentralized finance landscape, seamless integration with trusted third-party protocols augments both functionality and resilience. CyberGold champions such integrations, enhancing its core operations while steadfastly upholding its decentralized ethos.

Two pivotal off-chain functionalities are enabled through these third-party protocols: price feeds acquired via oracles and the optimization of asset utility through liquid staking.

Oracles, in their bridging capacity, channel external data into the blockchain. For CyberGold, this means obtaining the relative prices of the tracked asset (gold) and the backing asset (Ether). The choice for decentralized oracles[9] arises from their inherently distributed nature—data is sourced from various nodes, minimizing risks related to single points of failure and ensuring information reliability.

[9] The reference implementation leverages Chainlink.

Liquid Staking[10] allows CyberGold to utilize its backing assets, primarily Ether, within the proof-of-stake protocol, thereby contributing to the security of the underlying Ethereum ecosystem. This integration offers multiple benefits for the CyberGold ecosystem. Notably, it incentivizes more protocol insurers to participate, enhancing the protocol's robustness. As a result, stablecoin users enjoy increased stability.

Using third-party protocols introduces challenges, especially concerning sustainability and security. Both elements are vital for CyberGold's security. While CyberGold minimizes centralized risks, its functionality is linked to the reliability of these third-party systems. To counter potential issues, CyberGold has built-in mechanisms (in the form of various operational modes) ready to respond to any anomalies or threats.

2. Fully backed stablecoin

In the bustling realm of decentralized finance (DeFi), a myriad of stablecoins has emerged, all promising users an anchor of stability amidst the crypto world's inherent volatility. Though these stablecoins often make similar claims, their underlying mechanisms can be vastly different.

This chapter seeks to unravel the nuances of a fully backed stablecoin and underscores the significance of this backing mechanism. We will delve into how CyberGold consistently upholds the intrinsic value of its token, even when faced with turbulent market conditions, and the strategies it leverages to achieve this balance. Through this lens, our journey aims to demystify CyberGold's stability blueprint, accentuating its pivotal role in the DeFi ecosystem.

2.1. Asset-Backed Trust

Assets have long served as a safety net in financial transactions, acting as a cornerstone of trust and ensuring contractual obligations are met. This principle intensifies within the decentralized finance landscape. With limited intermediaries, assets backing financial instruments become paramount for trust and reliability.

While centralized stablecoins typically anchor their value by holding the tracked asset in off-chain reserves, crypto-backed stablecoins introduce a distinction between the tracked asset (e.g., USD or Gold) and the backing asset (such as Ether). Among these, some algorithmic stablecoins are particularly vulnerable, as their backing often relies on their project's own tokens. This model has seen several collapses due to "death spiral" scenarios, mirroring the pitfalls of Ponzi schemes[11].

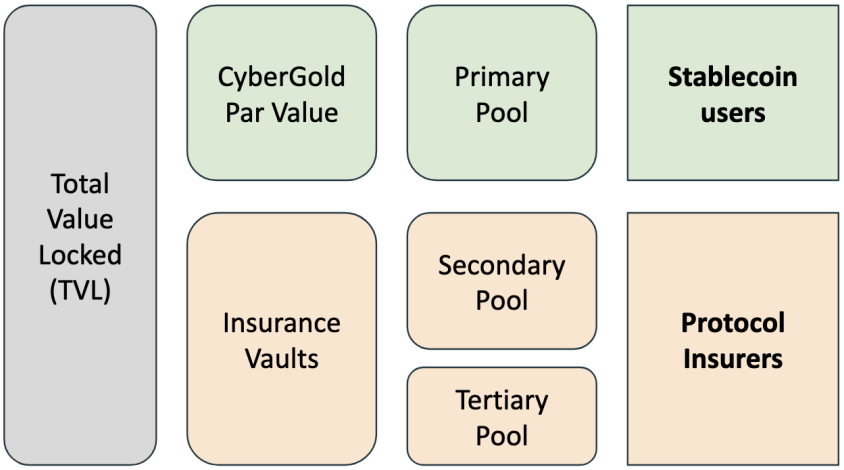
CyberGold, in contrast, is backed by Ether, a crypto-asset with a value independent of the CyberGold stablecoin. Central to its stability is the "PrimaryPool," meticulously managed to ensure its crypto-assets always match the par value of circulating CyberGold tokens. The

[10] The reference implementation leverages Lido.
[11] Cf. paper “Can the Stablecoins be stable?”

protocol ensures therefore constant solvency, guaranteeing that its inner value consistently matches its at-par value, showcasing steadfast reliability for its users.

2.2. The Triple-Layered Architecture of Backing

Ensuring unwavering stability in the tumultuous waters of crypto-assets demands an advanced design. CyberGold has pioneered a three-tiered pool system to fortify its solvency.



Triple-Layered Architecture of the CyberGold protocol

PrimaryPool: The Direct Equilibrium

The PrimaryPool serves as the bedrock of CyberGold's stability architecture. When users directly engage with the CyberGold issuance method, they are funding the PrimaryPool. In return, these users receive CyberGold tokens at a par value equivalent to the backing asset they provide. This pool crystallizes the direct correlation between the quantity of the stablecoin and its immediate collateral. Crafted meticulously, the value of the PrimaryPool, under normal circumstances, aligns with the par value of the circulating CyberGold tokens. A specialized rebalancing mechanism ensures its consistent alignment with CyberGold's outstanding liabilities.

SecondaryPool: The Resilient Buffer

Beyond the immediate backing lies the SecondaryPool, the domain of the risk bearers. These actors are incentivized to provide additional backing assets, especially crucial during adverse market dynamics, such as fluctuations in the exchange rate between the backed and the tracked assets. This pool serves as a protective layer, ensuring that despite market fluctuations, the integrity of the PrimaryPool remains uncompromised.

TertiaryPool: The Reward & Safety Net

The TertiaryPool serves a dual purpose in the CyberGold ecosystem. On the one hand, it acts as a reservoir for fees and staking rewards. These rewards and fees are designated for the risk bearers, who, who, as recognition for their pivotal role in upholding the protocol's stability, receive portions or shares of this pool. However, in the event that the SecondaryPool becomes depleted, the TertiaryPool stands as a last line of defense. Through the rebalancing mechanism, assets from this pool can be directed to maintain the integrity of the PrimaryPool.

2.3. Rebalancing Mechanism

The ever-changing dynamics of the crypto markets call for robust systems to preserve the stability of stablecoins. CyberGold's answer to this is a streamlined rebalancing mechanism that seamlessly harnesses real-time data and works in tandem with the protocol's multi-tiered pool structure. This section unpacks the workings of this mechanism, illustrating how it underpins the value of CyberGold, even amid market turbulence.

Price Determination

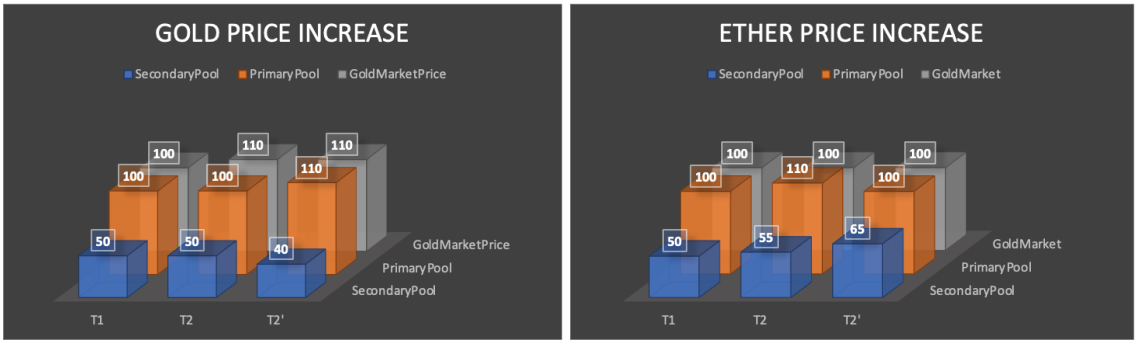
Central to the rebalancing mechanism is the accurate assessment of the tracking (gold) and backing (Ether) assets' relative value. To achieve this, CyberGold employs Chainlink price feeds—a reputable decentralized oracle system. This system offers timely and trustworthy data, playing an essential role in ensuring CyberGold stablecoin remains consistently pegged to gold, regardless of market vicissitudes.

The Rebalancing Mechanism Explained

At its heart, the rebalancing mechanism seeks to ensure that the value of the PrimaryPool always mirrors the circulating CyberGold tokens' par value. It achieves this by orchestrating seamless interactions between the different backing pools, especially during volatile market scenarios.

Whenever there's a significant shift in the relative value between the tracked asset (Gold) and the backing asset (Ether), such as when Ether declines or Gold appreciates, the PrimaryPool becomes undercapitalized in terms of its backing asset. To counteract this, the rebalancing mechanism is activated. Initially, it draws from the SecondaryPool to replenish the PrimaryPool. If the SecondaryPool is exhausted, the mechanism further accesses the TertiaryPool as an added safeguard. This systematic approach ensures that CyberGold remains fully backed, regardless of the relative fluctuations between Gold and Ether.

Conversely, when the relative value between the backing asset (Ether) and the tracked asset (Gold) increases in favor of Ether, the surplus value in the PrimaryPool is redirected into the SecondaryPool. This not only bolsters its reserves for potential future needs but also results in a leveraged profit position on the ETH-Gold conversion rate, benefiting the risk bearers.



The Rebalancing Mechanism in two scenarii.

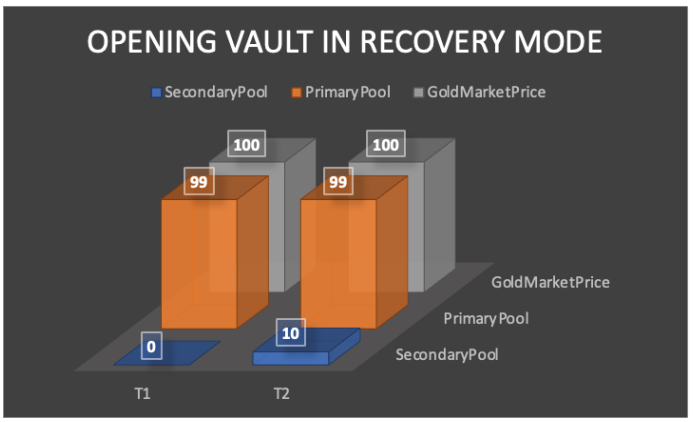
backingRatio Conservation Principle

At the heart of CyberGold's rebalancing strategy lies the 'backingRatio conservation principle'. This principle ensures that the rebalancing mechanism is dedicated to maintaining the previous backingRatio. To understand this ratio, one divides the value of the assets in the PrimaryPool by the par-value of the total circulating CyberGold tokens. Typically, this ratio stands at 1 during standard operation modes. However, there are instances in downgraded operation modes where this ratio might differ.

$$backingRatio = \frac{PrimaryPool}{StablecoinsSupply \times ExchangeRate}$$

This conservation approach serves a pivotal strategic function. If the SecondaryPool becomes depleted, it ensures that new protocol insurers can engage, without the risk that their contributions would be unfairly used up or drained.

In essence, the backingRatio conservation principle strengthens system integrity, fostering trust and ensuring that the protocol remains robust across varying market conditions.



The backingRatio conservation principle

3. Fully convertible stablecoin

In the expansive domain of stablecoins, the concept of full convertibility stands as an epitome of innovation and reliability. At its core, "full convertibility" signifies the unhampered and reciprocal ability to exchange Ether for its contemporaneous value in CyberGold, with only minimal issuance and redemption fees influencing the process. But such a potent feature doesn't exist in isolation—it's underpinned by CyberGold being "fully backed," a foundational principle elaborated upon in our prior chapter.

This transformative property ensures that users don't just pledge or collateralize their assets; they actively participate in a fluid exchange system. For users, the implications are monumental. They experience what can best be described as a direct currency swap, a testament to CyberGold's commitment to user-centric design and functionality.

Yet, as we will uncover in this chapter, full convertibility isn't just about straightforward exchanges. It's a principle that echoes through the very fabric of CyberGold, influencing its stability dynamics, capital efficiency, and the ebb and flow of its supply. In essence, full convertibility isn't merely a feature—it's a groundbreaking shift, reshaping how we perceive and interact with stablecoins in the decentralized finance landscape.

3.1. Full Convertibility and Stability

Central to CyberGold's value proposition is its inherent stability. This stability is directly championed by the principle of full convertibility. But how exactly does this convertibility translate to stability?

Imagine a scenario where the market price of CyberGold starts to diverge from its pegged value, which is bound to the universally recognized value of gold. Here’s where arbitrageurs step into the frame. They're always on the lookout for profit opportunities that arise due to price discrepancies.

For instance, should CyberGold trade at a price higher than its pegged value, an arbitrageur can purchase Ether, use it to issue new CyberGold tokens at the par value, and then sell these newly acquired tokens in the open market for a profit. Conversely, if CyberGold's market price falls below its pegged value, they can buy the CyberGold tokens from the market, redeem them for Ether at the protocol's guaranteed rate, and then sell the Ether for a profit. Through these actions, the arbitrageur not only profits from the price discrepancy but also nudges the market price of CyberGold back towards its pegged value.

Now, two critical mechanisms support this:

1. The **issuance mechanism** sets an upper bound, or a "ceiling", for the CyberGold price. It ensures that when the market price rises above the pegged value, new CyberGold tokens can be issued at par value, acting as a counterbalance.
2. The **redemption mechanism** establishes a lower bound, or a "floor". When the market price falls below the pegged value, the protocol promises to redeem CyberGold tokens at a rate equal (under standard operations) to its par value.

SCHEMA: 2 arbitrage cases

Small fees, resulting in a spread of +/- 1%, are charged for both issuance and redemption. This spread creates a buffer zone, ensuring that only significant price deviations attract arbitrage actions. Filtering out the noise of minor price deviations makes the system more resilient overall.

Lastly, CyberGold's decentralized nature offers an edge over traditional fiat-backed centralized stablecoins. Arbitrage opportunities can be acted upon 24/7, with no delays typically found in over-the-counter (OTC) transactions. By facilitating on-chain convertibility, CyberGold ensures uninterrupted access to its system. This round-the-clock operation, free from offline haggles or waiting periods, translates to market efficiency that stands second to none.

An inherent challenge in the world of trading is the market liquidity risk. In scenarios where market liquidity is low, the price of CyberGold might experience slippage, meaning it could move more than expected given a particular trade volume. But this is where the principle of full convertibility truly shines. Despite potential illiquidity, the continuous and instantaneous operation of CyberGold ensures that market forces, chiefly arbitrageurs (traders or bots), can swiftly intervene. By capitalizing on the price deviations, they guide the price back to its peg and restore equilibrium in the supply. It's a self-correcting mechanism, with the protocol's design actively ensuring that temporary liquidity constraints don't lead to prolonged price distortions.

In sum, full convertibility doesn't just promise stability; it actively harnesses market forces to ensure it.

3.2. Full Convertibility and Capital Efficiency

In the world of stablecoins, capital efficiency determines how optimally the underlying assets are utilized. At the heart of CyberGold's design is its unique approach to capital efficiency, anchored by the principle of full convertibility.

Many decentralized stablecoin protocols, such as DAI or LUSD, operate on an over-collateralized model. Here, users borrow stablecoins by depositing collateral that exceeds the borrowed value. Imagine depositing assets worth $150 to borrow a mere $100 worth of stablecoins. While this provides a cushion of stability and security, it does come with drawbacks. Not only does it tie up extra capital, but users must also constantly monitor their collateralization ratio to avoid the dreaded liquidation. This process can be both anxiety-inducing and time-consuming, especially during volatile market conditions.

CyberGold offers a refreshing departure from this model. Instead of navigating the intricacies of debt mechanisms, users can directly purchase CyberGold tokens at par-value, swapping Ether for CyberGold in a straightforward transaction. This ensures a 1:1 convertibility between the stablecoin and its backing asset, heralding optimal asset utilization.

In practical terms, with CyberGold, your assets get you an equivalent value in CyberGold tokens, without the overhead of excess collateral or the constant fear of liquidation. Every unit of value is actively engaged, maximizing the utility of each portion of capital. Therefore,

by eschewing the debt-laden issuance found in over-collateralized models, CyberGold stands as a pinnacle of efficient and user-friendly capital utilization.

3.3. Full Convertibility and Elastic Supply

Imagine a central bank that's not governed by bureaucracy, geopolitical tensions, or any human element. Instead, it operates solely on code and logic, making decisions with real-time data. This is the power behind CyberGold's fully decentralized central bank model, made possible by the principle of full convertibility.

Central to CyberGold’s architecture is its ability to maintain a dynamic balance between supply and demand, ensuring a seamless adaptability. The supply of CyberGold tokens isn't fixed or arbitrary. Rather, it's fluid, determined purely by market forces. Should there be an increased demand for CyberGold, the protocol allows for immediate issuance of new tokens, catering to this demand. Conversely, if demand decreases, tokens can be redeemed and removed from circulation. This ensures that CyberGold always mirrors the actual demand in the market, making its supply virtually unlimited. The only ceiling is the market capitalization of its backing asset, Ether.

To illustrate, consider two scenarios:

1. **Increased Demand**: The price of CyberGold rises above its peg due to heightened demand. Arbitrageurs spot the opportunity. They can instantly swap Ether for CyberGold using the protocol's issuance method, profiting from the price difference. This action increases the supply of CyberGold, restoring equilibrium.
2. **Decreased Demand**: The price of CyberGold drops below its peg because of diminished demand. Again, arbitrageurs come into play. They can redeem CyberGold for Ether through the protocol's redemption method, capitalizing on the price gap. This decreases the stablecoin's supply, steering it back to its peg.

Contrast this with over-collateralized stablecoins. Their supply is not primarily driven by the demand for the stablecoin itself but by borrowing activities. As users borrow against their collateral, new stablecoins are issued. This link between borrowing and supply may not always align with the actual demand for the stablecoin in the market.

Fiat-backed centralized stablecoins, which operate over-the-counter (OTC), don't offer the same fluidity as CyberGold. OTC operations, being manual and subject to human operational hours, can introduce delays. Such delays can result in discrepancies between actual demand and available supply.

CyberGold's model eliminates these inefficiencies. By automating its monetary policy through a decentralized mechanism, it ensures that its supply is always in sync with market demands, thereby offering a truly elastic and adaptable stablecoin solution.

Key Takeaways

- **Foundation of "Fully Backed"**: The core principle that enables CyberGold's full convertibility is its foundational property of being "fully backed." This guarantees that

for every CyberGold token in circulation, there is an equivalent value in backing crypto-assets held in reserve.

- **Stability through Convertibility**: CyberGold's full convertibility offers a self-regulating mechanism that uses market forces to keep the stablecoin close to its peg. This mechanism acts as a buffer against significant price fluctuations, providing users with confidence in the coin's stability.
- **Capital Efficiency**: By eliminating the need for over-collateralization, CyberGold ensures optimized asset utilization. Users benefit from direct 1:1 convertibility, avoiding the complexities and anxieties associated with potential liquidations prevalent in over-collateralized models.
- **Dynamic Elastic Supply**: CyberGold's supply is neither fixed nor arbitrary. Instead, it is determined by real-time market forces. This adaptability, governed by the protocol's decentralized nature, ensures that the supply of CyberGold always mirrors actual market demand. This contrasts with other models where supply may be influenced by borrowing activities or manual interventions.

In summary, the combined principles of "fully backed" and "full convertibility" underpin CyberGold's promise of stability, efficiency, and adaptability, distinguishing its approach within the broader stablecoin landscape in decentralized finance.

4. Fully liquid protocol

Amidst the myriad challenges of the decentralized finance ecosystem, the assurance of consistent liquidity remains paramount. Full protocol liquidity, which denotes a system's capacity to consistently offer an equivalent value for the stablecoins redeemed, is a cornerstone of trust for users. The CyberGold protocol uniquely navigates this space, seamlessly marrying the benefits of staking—with assets anchored to support network security—to an unyielding guarantee of liquidity. This chapter delves into CyberGold's adept approach to staking and its avant-garde techniques for upholding liquidity, even in the face of potential liquidity crises.

4.1. Liquid Staking

Before delving into CyberGold's approach, it's essential to understand the concept of staking within proof-of-stake (PoS) blockchain protocols. At its core, staking involves committing assets (or 'staking' them) to support network operations such as validating transactions and securing the network. Validators in a PoS system are chosen to create new blocks based on the number of assets they hold and are willing to 'stake' or lock up as collateral. In return for this commitment, they earn rewards.

Liquid staking is a groundbreaking mechanism in the blockchain space that overcomes limitations found in traditional staking methods. Essentially, it allows users to delegate their native blockchain coins (such as Ether) to validator nodes, bypassing the need to stake directly. In return for this delegation, users receive Liquid Staking Tokens (LSTs) that represent their staked position. This method eradicates the often high threshold of coins required to become a full validator and the challenges associated with operating a validation node. Moreover, it ensures enhanced liquidity as LSTs can be traded, used as collateral, or engaged in other decentralized finance (DeFi) activities.

4.2. Leveraging Liquid Staking in CyberGold

Liquid staking is a pivotal feature of the CyberGold protocol, with the majority of its backing assets, such as Ether, actively staked. This approach serves a strategic purpose: reinforcing the stability of the CyberGold stablecoin. The staking rewards underwrite the premiums of the insurance furnished by risk-bearers. It's a mutualistic arrangement: superior premiums correlate with enhanced hedging, elevating it beyond what would be gained from a straightforward leveraged position. As a positive side effect, the participation in the Proof-of-Stake consensus mechanism buttresses the stability of foundational Ethereum layer-1 protocol.

However, this strategy is not without challenges. Given that staked assets aren't inherently liquid, they introduce another layer of complexity in asset management.

4.3. Liquidity Management

At the heart of the CyberGold protocol's liquidity management lies a vital metric called the Liquidity Ratio, which is calculated using the following formula:

$$LiquidityRatio = \frac{unstakedAssets}{totalValueLocked}$$

Drawing an analogy from the traditional banking system, this ratio can be likened to the concept of fractional reserves. Just as banks keep a fraction of total deposits as reserve and allocate the rest for various investments, CyberGold aims to maintain a fraction of its assets in a liquid state while the majority remains staked. The protocol's approach to liquidity is guided by three distinct thresholds:

- **Target Threshold:** Analogous to a bank's reserve ratio, CyberGold consistently seeks to achieve a 15% liquidity ratio. This means that while 85% of the protocol's assets remain staked, 15% is kept liquid or unstaked, ready for immediate use.
- **Lower Bound:** Should the liquidity dip below a 10% threshold, the protocol triggers unstaking processes to restore the liquidity ratio to its target of 15%.
- **Upper Bound:** On the flip side, when liquidity exceeds 20%, the surplus assets are staked to align the ratio with its 15% target.

4.4. Handling Liquidity Crisis

While the protocol is designed to ensure availability of unstaked assets (Ether) under regular market conditions, it acknowledges the potential for exceptions like mass withdrawals. Although rare, these events are significant and can deplete the Ether reserves of the protocol. In such situations, instead of leaving users stranded, the CyberGold protocol provides them with Liquid Staking Tokens (LSTs), for an equivalent value.

This solution effectively handles the technical constraint of an inherent unstaking delay, giving users an alternative avenue to access the value of their assets. This approach mirrors a traditional banking response where, during a liquidity crunch, banks might offer customers illiquid financial assets, like treasury bonds, in lieu of cash. CyberGold's innovative approach provides a decentralized finance counterpart to this traditional safety net, mitigating liquidity risks and potentially averting full-blown liquidity crises.

While fiat-backed centralized stablecoins are vulnerable to bank run scenarios due to a lack of transparent backing or immediate liquidation mechanisms, CyberGold's decentralized approach offers a tangible and immediate solution through the provision of LSTs. This not only enhances user trust but also reinforces the protocol's resilience against such crises.

5. Protocol Insurers & Risk Hedging

CyberGold stands distinct in the crypto realm, not merely for its unique features, but for its innovative separation of roles. The **Stablecoin Users**, seeking stability, invest at par value and anchor CyberGold's immediate worth. Their objective is clear and straightforward: stability.

However, it is the **Protocol Insurers** who play a pivotal role in underpinning that stability. These insurers interact with the CyberGold protocol using "vaults," which are essentially NFTs representing their position within the system. These vaults detail their shares in both the SecondaryPool—funded initially by insurers and subsequently by surpluses from the PrimaryPool—and the TertiaryPool—which accumulates staking rewards and protocol fees. The Protocol Insurers interactions with the protocol is streamlined through specific vault operations: opening, escrowing, transferring, and closing.

In this chapter, we delve into the Protocol Insurers role and the vault operations, emphasizing their pivotal position within the CyberGold ecosystem.

5.1. Role and Responsibilities

The role of the Protocol Insurers is marked by its speculative nature. Such a role is tailor-made for investors with an in-depth comprehension of the protocol's mechanisms and the inherent risks accompanying it. While the allure of potentially lucrative rewards beckons, it is juxtaposed with considerable risks. To don the mantle of a protocol insurer is to embrace volatility and unpredictability.

Protocol Insurers are the bulwark against tumultuous market fluctuations. Their contributions to the SecondaryPool aren't mere capital injections; they're trust deposits ensuring the protocol's unwavering solvency and stability. In navigating the stormy seas of price volatility, they shoulder a responsibility that extends beyond personal gain. Their role is foundational, guaranteeing not just the solvency of the protocol but fortifying the stability of the entire ecosystem it supports.

Due to the inherent volatility of the crypto market and the complexities of the gold market, the exchange rate between Ethereum and gold can experience significant shifts. Given their leveraged position, these shifts can lead to substantial gains or, on the other hand, major losses. Thus, such a stance within the CyberGold ecosystem demands not only financial acumen but also a steadfast belief in the protocol's principles and potential, along with high confidence in the future movements of the Ethereum-to-gold exchange rate.

5.2. Motivations and Rewards

Protocol Insurers are motivated by a combination of both potential financial gains and their alignment with the broader objectives of the CyberGold protocol. The incentives drawing them to this speculative position can be broadly divided into leveraged opportunities and protocol-driven rewards.

Protocol Insurers are essentially in a "long" position when it comes to Ether, aiming to capitalize on a potential rise in its exchange rate against Gold. This position is intrinsically leveraged, meaning the potential gains (and losses) are amplified based on the dynamics of the CyberGold pools. The leverage they experience is quantified using the leverage ratio:

$$leverageRatio = \frac{totalValueLocked}{SecondaryPool}$$

Depending on the size dynamics between the PrimaryPool and the SecondaryPool, this ratio can vary, emphasizing the need for Risk Bearers to exercise prudence and astute financial judgment.

Beyond the potential gains from their leveraged position, Protocol Insurers also benefit from the protocol's rewards system. The TertiaryPool, which accumulates protocol fees and staking rewards, allocates "stocks" to the Protocol Insurers, that are encoded within the NFTs representing their vaults. The magnitude of each share is determined proportionally based on the insurer's initial investment amount and the escrow duration. As the protocol grows and more transactions take place, these rewards can serve as a significant incentive for the insurers, providing a consistent flow of benefits for their commitment to the system.

In navigating the intricate balance between potential high returns and inherent risks, these incentives offer Protocol Insurers a comprehensive and multi-faceted reward structure, reinforcing their pivotal role in the CyberGold ecosystem.

5.3. Vaults operations

For Protocol Insurers, the CyberGold protocol offers four main vault operations: opening, escrowing, transferring, and closing. Each vault is uniquely represented in the form of a standardized non-fungible token (NFT), embedding metadata detailing:

- Stocks owned in the SecondaryPool,
- Stocks owned in the TertiaryPool,
- The escrowing period's end date.

The decision to represent vaults as NFTs was strategically rooted in safeguarding the system against misuse. By leveraging the inherent non-fungibility of NFTs, the vaults are precluded from being traded on conventional exchanges, thereby reducing the potential for inexperienced individual investors to inadvertently expose themselves to the instrument's intrinsic risks. However, this design does not eliminate trading altogether; it merely redirects it to specialized NFT marketplaces, ensuring a more informed and intentional trading environment.

Vault opening

At the outset of the vault opening process, a Protocol Insurer commits additional "backing assets" (in the form of Ether) to the CyberGold protocol. In reciprocation for this commitment, they receive a unique NFT symbolizing their vault, that is minted during the process.

Concurrent with the creation of the vault, the Protocol Insurer is ascribed a proportional stake from the SecondaryPool. This allocation, which mirrors the value of the contributed

Ether in comparison to the entirety of the SecondaryPool, is embedded within the NFT's metadata. The formula for determining this allocation is:

```
if secondaryPool != 0:
```

$$secondaryStocks = \frac{initialDeposit}{secondaryPool} \times totalSecondaryStocks$$

```
else:
```

$$secondaryStocks = initialDeposit$$

Vault escrowing

At opening, the vault has to be escrowed for a minimum duration of 1 month (and up to 12 months). This minimum escrowing period, set to one month, is an essential safeguard as it serves as a deterrent against certain oracle front-running attacks. Moreover, the selection of the escrow period is crucial as it directly influences the stocks allocation from the TertiaryPool (therefore on the fees and staking rewards generated by the protocol). More precisely, the stocks received from the TertiaryPool are proportional to the amount escrowed. Additionally, the amount of stocks increases based on the duration of the escrowing raised to a specific power. This means that the longer the vault is escrowed, the more stocks are received at an accelerating rate. Here is the formula :

$$tertiaryStocks = \frac{initialDeposit}{secondaryPool} \times escrowDuration^{escrowingPower}$$

Later, and even before the expiration of the escrowing period, one can renew or prolong the escrowing period of its vault. Therefore, the Protocol Insurer will increase its stocks of the TertiaryPool.

Escrowing vault demonstrates a long-term engagement toward security of the protocol. Notice that, even if a vault is escrowed and can’t be closed, it can still be transferred.

Vault transfer

Protocol Insurers are endowed with the possibility to transfer their vaults, even before the vault maturity, enabling a layer of flexibility and liquidity. While these vaults, represented by NFTs, are intrinsically tied to the protocol’s stability mechanisms, allowing their transfer does not compromise the hedging integrity of the CyberGold system. Instead, it offers Insurers an avenue to manage their positions more dynamically.

Vaults, as any ERC-721 compliant NFTs, can be transferred in different ways: such as directly through a peer-to-peer exchange or via established NFT marketplaces. In essence, it's a thoughtful balance between ensuring the protocol's robustness and granting flexibility to its stakeholders.

Vault closing

Upon reaching maturity, Protocol Insurers have the option to close their vaults. This process involves the conversion of the stocks linked to their NFT back into Ether, reflecting the initial investment and any earned entitlements from the protocol's pools.

The Ether amount to be redeemed from the SecondaryPool is calculated using the following formula:

$$Ether\_from\_Secondary = (\frac{secondaryStocks}{totalSecondaryStocks}) \times secondaryPool$$

Similarly, the Ether equivalent from the TertiaryPool is given by:

$$Ether\_from\_Tertiary = (\frac{tertiaryPoolStocks}{totalTertiaryPoolStocks}) \times tertiaryPool$$

Summing the results from both formulas will give the total Ether amount due to the Protocol Insurer upon vault closure.

As a final step in the closing process, the associated NFT will be permanently burned. Closing a vault is not just a procedural task; it signifies the end of an insurer's commitment to a specific vault, converting virtual assets and entitlements back into tangible assets in the form of Ether.

5.4. Market-driven hedging ratio

Unlike some financial protocols that rely on predetermined, static figures, the CyberGold system does not utilize a hard-coded optimal hedging ratio. Instead, it adopts a more organic approach, allowing the hedging ratio to be dynamically determined by market forces.

The beauty of this approach lies in its self-regulation. As the reserve funds decrease, the incentive structures are designed to intensify, ensuring that the hedging ratio never dwindles to zero. This dynamic interaction between the reserve funds and incentives guarantees the protocol's resilience and adaptability.

Every market price, at its core, is a balancing act. It reflects an equilibrium between bullish ("long") and bearish ("short") market sentiments. This balance arises from the interplay of demand and supply, from sellers and buyers, each vying to shape the asset's price trajectory. In the context of the CyberGold protocol, this equilibrium provides a constant, ever-shifting dance of probabilities, where the chance of the backing asset (Ether) appreciating or depreciating against the tracked asset (gold) remains evenly poised. It is against this backdrop of uncertainty and potential that the protocol's insurers place their bets, predominantly aligning with those who anticipate a rise in Ether's value relative to gold.

5.5. Financial risks

Protocol insurance within the CyberGold system embodies a sophisticated financial instrument, layered with intricacies and potential pitfalls. Before delving into this realm, it's essential to understand and appreciate the risks fully.

1. **Protocol Complexity:** Protocol insurance hinges on the multifaceted CyberGold protocol. Thorough comprehension is crucial, as a lack of it can lead to potential missteps.
2. **Leverage and Market Dynamics Risks**: Protocol Insurers operate in a leveraged position. This amplifies not only potential gains but also the susceptibility to losses, especially when market dynamics are volatile. A robust risk management strategy is therefore essential.
3. **Liquidity Constraints:** Insurance vaults within CyberGold may be less liquid due to escrow periods and non-fungible tokenization, limiting rapid asset movements in fluctuating markets.

Key Takeaways

The innovative CyberGold protocol stands out with its distinctive separation of roles, ensuring stability within the crypto realm. At its core, the system is anchored by the interplay of two key players. The Stablecoin Users anchor CyberGold's value by investing at par value with their primary desire being stability. On the other hand, Protocol Insurers, are the risk bearers who bolster this stability. Protocol Insurers interact with the system through "vaults", unique NFTs that detail their stocks in the Secondary and Tertiary Backing Pools. These vaults facilitate a range of operations such as opening, escrowing, transferring, and closing. The representation of vaults as NFTs serves to protect the system from misuse, ensuring that trading is contained within specialized NFT marketplaces or direct trading, and away from conventional exchanges.

Protocol Insurers, while pivotal, also shoulder considerable risks, stemming from market dynamics and the protocol's complexities. As such, any potential investor must approach with a well-informed perspective, armed with thorough research and understanding. Their role, however, is not unrewarded. They stand to gain from the protocol's reward system and the potential rise of Ether's exchange rate against Gold.

This design creates a market-driven hedging ratio – a dynamic, self-regulating aspect of the CyberGold system which adjusts organically as per market forces to embody the protocol's adaptability and resilience.

6. Fees and Operational Modes

Like the precise gears of a masterfully crafted watch, the meticulously structured fee system and a series of operational modes of CyberGold determine the protocol's resilience and adaptability. Tailored to navigate various market conditions, these design elements ensure that CyberGold remains stable, user-friendly, and primed for real-world utility.

This chapter will delve deep into the integral roles of both fees and operational modes. First, we'll navigate the layered fee structure, understanding its dual purpose: to protect against potential vulnerabilities and to fuel the engine of incentives that keeps the protocol's stakeholders engaged. Following this, we'll transition into the realm of operational modes. Each mode, from Standard to Exit, represents a unique strategy designed to adapt and respond to different market challenges, always with the aim to protect and serve CyberGold's user base.

By the end of this chapter, you will gain a holistic understanding of how the CyberGold protocol utilizes these mechanisms not just as operational necessities but as strategic tools, ensuring its longevity and relevance in an ever-evolving market landscape.

6.1. The Purpose and Design of Fees

The stability and functionality often rest on foundational mechanics, and the CyberGold protocol is no exception. It's essential to note that the fees in this system serve two interconnected reasons. First, on a technical level, they shield the protocol from front-running attacks, particularly those targeting oracles. These attacks, if unchecked, can skew asset values and threaten the protocol's integrity. The CyberGold protocol has cleverly calibrated its issuance and redemption fees in accordance with the deviation threshold used by the third-party oracle price feed, to make such malicious endeavors financially unviable.

Secondly, these fees serve as the linchpin for economic synergy within the protocol. They act to incentivize the risk-bearers, who, in return for shouldering certain risks, benefit from these collected fees. Thus, they can be viewed as insurance premiums, paid by CyberGold users to the risk-bearers to ensure stability. By offering a rewarding proposition for insurers, the system tightly aligns their interests with those of the CyberGold protocol.

It is to notice that a fee system does introduce a spread, a slight difference between issuance and redemption prices. While this may seem counterintuitive for a system prioritizing stability, it's a measured trade-off. This spread ensures that the market price will operate within a narrow corridor, and ensures that arbitrageurs only come into play when there are substantial deviations from the peg.

Adopting a flat fee system is a deliberate choice by the CyberGold protocol. The advantages of this approach are numerous. With flat fees, users are provided a low spread and shielded from the risk of slippage when interacting with the protocol. This straightforward structure ensures predictability, making it simpler for users to forecast costs.

From a design perspective, flat fees are not just user-friendly but also system-efficient. They are more straightforward to implement and ensure optimal resource utilization, translating into gas efficiency. The decision to peg these fees to the deviation threshold of the oracle price feed ensures they remain both fair and adaptable, catering to the dynamic nature of crypto markets.

With a clearer understanding of how fees anchor the system, it's also crucial to note their variance across operational modes, a testament to the protocol's adaptability.

6.2. Operational Modes

In the cryptocurrency wilderness, it's not the strongest that thrive, but those most responsive to change. Protocols that can't dynamically adjust to market conditions, third-party risks, and looming cyber threats risk extinction in this relentless ecosystem. For governance-free protocols like CyberGold, this Darwinian principle of adaptability is paramount. Recognizing this, the CyberGold protocol is designed with three distinct operational modes. Each mode is tailored to specific market conditions, with an automated activation mechanism based on the state of the protocol, predominantly dictated by the backingRatio value (cf. section 2.3). The intent is always clear: to preserve the protocol's integrity, protect its users, and ensure continued operation.

Standard Mode

In the ideal state of the protocol, when the backing ratio is precisely one, we find the CyberGold protocol operating in its Standard Mode. During this phase, the system allows all operations for both users and insurers without restrictions. The fees and staking rewards collected are channeled toward the TertiaryPool. By doing so, the protocol ensures a constant reward mechanism that serves the community and keeps stakeholders engaged.

Recovery Mode

When the waters become slightly choppy and the backing ratio drifts to fall between 0.9 and 1, the protocol switches to Recovery Mode. This mode has a clear-cut mission: to reclaim the peg with the underlying asset, gold.

In Recovery Mode, the fee structure undergoes a change, becoming slightly steeper than in Standard Mode. This is a deliberate measure, taken to expedite the recovery of the peg. Furthermore, these heightened fees are redirected, not to the TertiaryPool, but to replenish the PrimaryPool. This redirection reinforces the protocol's resilience and primes it for a swift return to its optimal state. Users should be aware that in Recovery Mode, while all operations remain possible, redemptions might not yield the full par value, as the protocol's solvency may be in question. Instead, users receive a proportionate share of the backing assets housed in the PrimaryPool:

$$etherAmountReturned = stablecoinsRedeemed \times \frac{backingRatio}{GoldToEtherExchangeRate}$$

Exit Mode

The Exit Mode is the CyberGold protocol's emergency exit. Triggered when the backing ratio plummets below 0.9, this mode exists to ensure stakeholders, particularly CyberGold stablecoin holders, can exit the protocol with the least possible loss. This mode is the protocol's final defensive strategy against unanticipated challenges or potential hazards. A critical trigger for this mode, besides the low backing ratio, is an abnormal delay in updating the oracle—specifically, a delay that's twice the oracle's standard "heartbeat" duration.

Unlike the other modes, Exit Mode waives all fees. The focus here is not on operations but on safeguarding stakeholder interests. While issuing new CyberGold tokens is halted, users retain the ability to redeem existing tokens. However, as in the Recovery Mode, redemption might yield less than the par value, since the protocol's solvency may be compromised in Exit Mode. In this mode, the vault opening operation is suspended.

Key Takeaways

Understanding the operational modes of the CyberGold protocol is key to comprehending its adaptability and commitment to user protection. To simplify:

Operational Mode	**Trigger Condition**	**Primary Objective**	**Fee Direction**
Standard	backingRatio = 1	Optimal operations for all stakeholders	TertiaryPool
Recovery	0.9 ≤ backingRatio < 1	Reclaim peg with the underlying asset (gold)	PrimaryPool
Exit	backingRatio < 0.9 or oracle delay	Safeguard stakeholders and allow exit with minimal losses	No fees collected

This dynamic structure not only adds layers of security to the CyberGold protocol but also underlines its dedication to stability, flexibility, and user protection in a fluctuating crypto market.

7. Risks and Mitigations

Blending the timeless value of gold and the advantages of digital assets represents a significant leap forward, yet it also ushers in a suite of risks that demand both acknowledgment and meticulous management. Decentralized systems, despite their transformative potential, are intricately layered with challenges, each with its own nuances. From third-party dependencies to the inherent market volatilities, the terrain is dotted with potential pitfalls that could impact the security and trust in the protocol.

Yet, recognizing these challenges is the first step in crafting a resilient protocol. It's crucial to understand that while we employ best-of-class strategies to mitigate these risks, the landscape of decentralized finance doesn't allow for a zero-risk environment. However, what the CyberGold protocol promises is a relentless commitment to transparency, and the deployment of robust measures designed to limit both the occurrence and impact of these risks.

It's worth noting that while we might have touched upon some of these risks in preceding chapters, this section stands as a comprehensive repository. Here, we not only reiterate these challenges but also stringently outline all the countermeasures the CyberGold protocol has in place. As you journey through this analysis, you'll gain a comprehensive understanding of our dedication to securing the CyberGold ecosystem, all while acknowledging the inherent challenges of this frontier.

7.1. Exchange Rate Risk

Given the inherent volatility of exchange rates between diverse assets, the CyberGold protocol is specifically designed to tackle the Exchange Rate Risk, which emerges when Ether's value declines relative to Gold.

Our protocol employs a robust "rebalancing mechanism" that transfers the risk from stablecoin users to protocol insurers, acting as the protocol's bulwark and bearing the financial repercussions of fluctuations in the exchange rate between Ether and Gold. Due to their leveraged position, protocol insurers may encounter substantial financial losses. However, as long as this price decline remains slow or moderate, the protocol design ensures that the stablecoin's peg to Gold remains defended. The only tangible drawback effect for the protocol in such instances would be a transient decrease in the hedging ratio.

Nevertheless, it's essential to understand that the efficacy of this stability insurance has its limits. Should Ether face a profound and sudden drop in value compared to Gold, the safety measures might be strained, endangering the stablecoin's peg to Gold. In such extreme scenarios, the SecondaryPool and TertiaryPool might be depleted, leading to insurers losing their entire investments and eroding the protocol's security layers. At this juncture, the protocol is geared to activate either the recovery mode or the exit mode. These strategies aim to either restore the peg or enable a regulated exit for stablecoin users with minimal losses, emphasizing the system's inherent resilience.

7.2. Low Hedging Risk

Inextricably tied to Exchange Rate Risk is the phenomenon of Low Hedging Risk. We've already discussed how the Exchange Rate Risk is offset by the hedging provided by the protocol insurers. However, this safeguard's effectiveness hinges on the protocol's hedging ratio, which essentially measures the relative sizes of the SecondaryPool and TertiaryPool against the total reserves of backing assets. Given that the hedging ratio is determined by market dynamics, it's imperative for the protocol to perpetually incentivize an optimal hedging ratio, which represents the percentage of relative price drop that the current reserves could absorb:

$$hedgingRatio = \frac{SecondaryPool + TertiaryPool}{PrimaryPool + SecondaryPool + TertiaryPool}$$

To achieve this, several strategies are in play.

Firstly, in standard operation mode, all fees and staking rewards are channeled as premiums to bolster the protocol's security. This mechanism not only incentivizes protocol insurers but does so more aggressively when the hedging ratio dips — precisely when augmented protection becomes paramount.

Next, the escrowing of solvency insurers' vaults fosters a long-term allegiance to the protocol. This escrow acts as a deterrent, preventing protocol insurers from withdrawing from the protocol during volatile periods, ensuring their unwavering support when it's critically needed.

Lastly, the protocol implements the "backingRatio conservation" principle (cf section 2.3). This principle, fundamental to the rebalancing mechanism, aims to preserve the pre-existing backing ratio. This ensures that incoming risk bearers can confidently participate since their contributions are protected from instant depletion when the protocol is navigating its recovery mode.

7.3. Third-Party Risk

The CyberGold protocol, while a robust entity in its own right, relies on certain third-party services to function seamlessly. This reliance naturally introduces what we term as the 'Third-Party Risk'. Two main third-party services that the protocol hinges upon are the oracle services (which provide the price feed) and the liquid staking protocol.

The role of an oracle service is pivotal. It provides real-time data (price feeds in our case) that inform many of the protocol's operational decisions. If the oracle service fails, it can jeopardize the stability and accuracy of the CyberGold protocol. In particular, if there's no update from the oracle during a predetermined timelapse (called 'oracle heartbeat'), that could signal a potential malfunction or compromise. Consequently, the Exit Mode will be triggered.

The rationale for using the liquid staking protocol is to increase the incentives for protocol insurers, and therefore to increase the hedging ratio. Nevertheless, Liquid Staking Tokens (LSTs) have their own set of market dynamics and can be influenced by various factors external to the CyberGold protocol. If the value of LSTs were to drop below the par-value, it could strain the liquidity of the protocol and destabilize its operations. Recognizing this vulnerability, the CyberGold protocol has a preemptive measure in place. Should the price of LSTs significantly fall below the par-value, the protocol would suspend all liquid staking operations. This action halts potential cascading negative effects and stabilizes the protocol, preventing any further risk exposure to users and insurers.

In summary, while Third-Party Risks are inherent given the interconnected nature of blockchain protocols, the CyberGold design continually monitors, reacts, and adapts to these potential hazards, ensuring that the interests of all stakeholders are front and center in every decision made.

7.4. Smart Contract Risk

Decentralized finance hinges upon the trustworthiness of smart contracts. These pieces of code, while powerful, can sometimes be vulnerable to certain exploits if not rigorously tested and verified. Recognizing this, the CyberGold protocol places utmost priority on ensuring its smart contract remains resilient against all known threats.

Our commitment to security is evidenced in multiple ways:

1. **Open-Sourcing**: By open-sourcing the code, we invite the global community to inspect, evaluate, and contribute to our protocol. This communal scrutiny acts as a safeguard, ensuring no lapses are overlooked.
2. **Audits**: Security audits conducted by reputed third-party security firms are ensuring that our protocol stands up to the highest standards of security in the industry.
3. **Formal Verification**: Beyond conventional testing, our smart contracts undergo formal verification. This mathematical approach ensures that the contract will behave as intended under every possible condition.
4. **Stress-Testing and Bug Bounties**: During our extensive stress-testing period, we not only simulate high-stress scenarios and potential attack vectors but also implement bug bounties. By incentivizing the community to identify vulnerabilities, we harness collective expertise to further fortify our system.

Despite these precautions, it's imperative to acknowledge that no smart contract can be proven invulnerable— a fact that becomes painfully obvious the exact moment it's hacked. In the event of an unexpected security breach, the CyberGold protocol has a fail-safe in place: the Exit Mode. This mechanism acts as the final defense line, aiming to ensure a well-organized and structured exit from the protocol for its users, striving to preserve and return as much of their assets as possible.

7.5. Reserve Liquidity Risk

In the realm of stablecoins, the stability and trust in the system often hinge on the peg these coins maintain with a stable asset. At the heart of this peg is the premise: for every stablecoin in circulation, there's an equivalent reserve held by the issuer, ready to be liquidated should holders wish to redeem their coins. Yet, what if a sudden rush – akin to a bank run or market downturn – saw a large fraction of holders demanding their reserve asset simultaneously? This scenario poses the reserve liquidity risk. Should the issuer be unable to satisfy these redemptions, confidence in the stablecoin might wane, potentially pushing its value below the intended peg.

CyberGold navigates this terrain with a two-pronged reserve approach. Firstly, there are liquid assets in the form of the primary backing asset: Ether. These provide direct liquidity. Parallel to this, there's a secondary, less liquid reservoir: Liquid Staking Tokens (LSTs), which are procured by staking Ether on the liquid staking protocol. In an innovative maneuver to counteract liquidity crises, CyberGold offers the possibility of disbursing LSTs instead of Ether. By incorporating this mechanism, CyberGold presents a forward-thinking strategy to assuage reserve liquidity risks, striving to ensure that stablecoin users can always withdraw, even during a bank-run scenario.

7.6. Market Liquidity Risk

A resilient stablecoin is characterized by its unwavering price stability, even when faced with significant trading movements. Market liquidity risk emerges when trading actions, even of modest volumes, can inadvertently shift the coin's price, dislodging it from its peg. This challenge is especially pronounced for stablecoins that operate with a smaller market capitalization or trading volume.

Arbitrage is central to CyberGold's strategy for managing this risk. Although liquidity gaps may occasionally arise, the full convertibility property combined by continuous operations of the CyberGold protocol ensures that arbitrageurs can act without delay. By capitalizing on price discrepancies, they bring the stablecoin's price back in line with its peg, re-establishing a balanced supply-demand relationship. This self-regulating mechanism guarantees that short-term liquidity issues don't turn into sustained price deviations.

In the early stages of the protocol, dedicated arbitrage bots will have a pivotal role in ensuring that the CyberGold stablecoin's price remains tethered to the value of Gold across both decentralized exchanges (DEX) and centralized ones (CEX). It's not merely a passive reliance on market forces; CyberGold proactively nurtures this equilibrium right from its inception, making certain the stablecoin remains consistently anchored.

7.7. Financial Loss Risk

For participants in the CyberGold ecosystem, financial loss risks manifest in diverse ways. It is therefore imperative for participants to understand and evaluate the financial implications inherent to their roles within the ecosystem.

Stablecoin Users: Their primary exposure stems from a potential decline in the value of the tracked asset, Gold, in comparison to other assets. For instance, if Ether (the backing asset) appreciates significantly relative to Gold, users might experience an opportunity loss. Furthermore, from a broader financial perspective, there's also the risk tied to fluctuations between Gold and users' national currencies. Such movements can impact the real-world purchasing power of their holdings.

Protocol Insurers: These stakeholders grapple with the opposite side of the coin. Their concern centers around the depreciation of the backing asset (Ether) in comparison to the tracked asset (Gold). Given their leveraged positions within the protocol, even marginal declines can amplify their financial exposure, culminating in substantial losses.

7.8. Legal Risk

Navigating the world of decentralized finance requires not just technological savvy, but also a nuanced understanding of legal implications. The CyberGold protocol, while pioneering in its offerings, is not exempt from the realm of legal considerations.

All involved parties, whether they be smart-contract deployers, front-end operators, stablecoin users, or protocol insurers, bear the responsibility of ensuring their interactions with the CyberGold protocol align with the legal frameworks of their respective jurisdictions. This encompasses a broad spectrum of regulations including but not limited to Know Your Customer (KYC) norms, Anti-Money Laundering (AML) directives, and securities regulations.

Legal Disclaimer: It's paramount to note that while the CyberGold protocol is engineered with the utmost precision and diligence, it doesn't provide legal counsel. All users, regardless of their role within the ecosystem, are strongly urged to seek professional legal advice tailored to their specific circumstances. Ensuring compliance and legal clarity not only safeguards individual actors but also fortifies the integrity and longevity of the CyberGold ecosystem as a whole.

Key Takeaways

Risks	Primary Mitigation Strategies
Exchange Rate Risk	- Rebalancing mechanism that transfers risk to protocol insurers. - Activation of recovery or exit mode in extreme scenarios.

Low Hedging Risk	- Channeling all available resources as premiums. - Escrowing of solvency insurers' vaults. - backingRatio conservation principle.
Third-Party Risk	- Exit Mode activation for oracle delay. - Suspension of liquid staking operations if LSTs fall below par-value.
Smart Contract Risk	- Open-sourcing code. - Regular audits. - Formal verification. - Stress-testing and bug bounties. - Activation of recovery or exit mode in case of unexpected breach.
Reserve Liquidity Risk	- Possibility of disbursing LSTs instead of Ether.
Market Liquidity Risk	- Active arbitrage mechanism (enhanced by full convertibility and continuous operations) - Dedicated arbitrage bots
Financial Loss Risk	- Educating participants about the financial implications based on their roles in the ecosystem.
Legal Risk	- Encourage all parties to adhere to legal frameworks of their jurisdictions. - Strongly urge seeking professional legal advice.

8. Miscellaneous

In our journey of designing and presenting this protocol, we've come across several essential aspects that might not fit squarely into the specific technical or operational categories previously discussed, yet are vital for a comprehensive understanding. This chapter sheds light on some of these miscellaneous, but equally significant, aspects. From our protocol's environmental footprint to the legal nuances and the specifics of our reference implementation, we aim to present a holistic view. Let's delve into these details.

8.1. Environmental Impact

The environment's well-being remains a growing concern in the world of technology. It's essential to emphasize that the reference implementation of our protocol was designed for the Ethereum blockchain, which has adopted the proof-of-stake consensus. Notably, this consensus mechanism is substantially more energy-efficient than its counterpart, proof-of-work, used by other blockchains like Bitcoin. To put it in perspective, the proof-of-stake consensus is approximately 30’000 times more efficient[12], aligning with our commitment to a greener planet.

8.2. Legal Disclaimer

Purpose, Scope, and Reference Implementation

The protocol, accompanied by its associated reference implementation, is crafted and provided exclusively for academic and research applications. The Cifero organization's role is limited to designing the protocol and offering a reference implementation. We do not support, endorse, or encourage the deployment or usage of this protocol on any blockchain mainnet. Moreover, Cifero explicitly absolves itself from any responsibility or liability related to potential deployments and the ensuing consequences or ramifications of such actions.

Liability Limitations:

For users who choose to interact with implementations of the protocol on mainnet against our advice, we will not be held responsible or liable for:

1. Regulatory non-compliance in the user's jurisdiction.
2. Financial losses or other consequential damages.
3. Potential software bugs, data breaches, or other security vulnerabilities.
4. Unexpected behavior or outcomes resulting from protocol interactions.
5. Compatibility issues with other software or protocols.

Financial Product Notice

Users should recognize that not only deploying the protocol but also any form of interaction with an instance of this protocol on a mainnet—including operating a front-end application,

[12] Ethereum Energy Consumption | ethereum.org

utilizing the CyberGold stablecoins, or investing in the insurance vaults—might run afoul of regulatory frameworks. This includes but is not limited to guidelines specific to KYC, AML, and securities in their respective jurisdictions. Nevertheless, if the protocol were to be deployed, the financial structured products associated with it would be designed primarily for qualified investors. Therefore, comprehensive adjustments and thorough due diligence are imperative prior to any form of engagement.

Not Financial Advice

The information contained herein does not constitute financial or investment advice. All users are urged to use this service responsibly and seek independent advice as necessary.

8.3. Reference Implementation

Here is a table detailing the constant values integral to its functioning:

Parameter	Value
Base Fee Rate	1%
EscrowingPower	1.5
Lower Bound for Liquidity Ratio	10%
Target for Liquidity Ratio	15%
Upper Bound for Liquidity Ratio	20%
Bounds for Activating the Exit Mode	90%

And here is an overview of the protocol fees for the various operations in each mode:

	Stablecoin Operations			Vault Operations			
Operational Mode	**Issuance**	**Redemption**	**Transfer**	**Opening**	**Escrowing**	**Transfer**	**Closing**
Standard	1%	1%	0%	0%	0%	0%	0%
Recovery	2%	2%	0%	0%	0%	0%	0%
Exit	Disabled	0%	0%	Disabled	0%	0%	0%

8.4. Licence

As a non-profit entity driven by community contributions, we've chosen to license our code under the **GNU General Public License (GPL)**. This decision aligns with our commitment to promoting open-source code and ensuring that any derivative work remains in the public domain, benefitting the broader community. The GPL prevents private and commercial entities from restricting the code's distribution, ensuring the protocol's essence remains consistent and accessible to all.

Key Takeaways

In wrapping up this chapter, it's evident that the intricacies of our protocol extend beyond its technical and operational facets. From prioritizing environmental sustainability to promoting transparency and open-source ethos, the Cifero organization remains committed to responsible and inclusive development. While the topics in this chapter varied, they collectively underscore our dedication to building a protocol that stands up to scrutiny, is accessible to all, and aligns with the broader goals of community and sustainability.

Conclusion

The intricate world of decentralized finance is marked by continuous innovation, and the CyberGold protocol stands as a testament to this evolution. Drawing inspiration from both historical antecedents and modern advancements, it seeks to chart a distinctive path in the crypto landscape. In this concluding chapter, we don't aim to plunge anew into the intricate details, but rather to take a step back, drawing together the threads of our discussion from earlier chapters. Join us in reflecting on the core concepts, the challenges faced, and the broader potential implications of the CyberGold protocol in the overarching story of digital finance.

A. Recapitulation of CyberGold Protocol

Anchored in the ideals of the cypherpunk movement, the CyberGold protocol was crafted with a vision of fostering greater financial autonomy. With its commitment to decentralization, it leverages blockchain technology, guided by the not-for-profit ethos embodied by Cifero. This harmonious blend holds the potential to offer a refreshing perspective in the stablecoin domain, emphasizing trustworthiness, clarity, and shared governance.

At its core, CyberGold boasts several distinguishing characteristics:

- **Trustless protocol**: governance-free protocol, censorship resistant
- **Common good**: decentralized protocol, non-profit monetary system
- **Gold standard**: stablecoins are pegged to gold, a time-tested and decentralized asset
- **Fully backed**: stablecoin's value is fully stored in reserves in the form of crypto-asset (Ether)
- **Fully convertible**: users can directly swap stablecoins and Ether (and vice-versa)
- **Capital efficient**: optimal efficiency due to the dual-role architecture
- **Responsive supply**: the supply dynamically adjusts to the stablecoin demand

In synthesizing these elements, CyberGold has crafted a robust, reliable, and responsive financial protocol, set to inject fresh momentum into the crypto space.

B. Legacy

The heart of the CyberGold protocol is deeply entrenched in its open-source foundations. This commitment to transparency and collaboration isn't just about codes and algorithms but also about fostering a culture where innovation is not just encouraged but celebrated. In the fast-paced realm of digital finance, projects like CyberGold, with their open doors and shared insights, can lead the way, promoting collective progress over isolated feats.

This era of digital currency isn't born in a vacuum. As we mark 15 years since the publication of the Bitcoin White Paper, there’s a need to tip our hats to the trailblazers. While Cifero carries its own distinct mission and methodology, it does so while cherishing the foundational spirit that Bitcoin introduced: decentralization, empowerment, and revolutionizing the

traditional. Every step CyberGold takes is a nod to these initial ideals, even as it carves its own path forward.

Amidst the tumultuous ebb and flow of the crypto world, there's a palpable yearning for stability. The volatile highs and lows of cryptocurrencies present challenges, but also opportunities. In this landscape, CyberGold emerges with hope, not as a panacea, but as a stabilizing force. With its unique operational mechanics, it aspires to provide a steadying influence, creating ripples that might help bring more predictability and assurance to the broader digital economy.

In the ever-evolving story of digital finance, CyberGold’s contributions, be they monumental or modest, add a new chapter of relentless innovation and a pursuit of a stable, reliable digital future.

C. Future Perspectives

The decentralized finance landscape stands at a crossroads, facing both immense challenges and unprecedented potential. While the vision of mainstream DeFi adoption is alluring, it grapples with technological entry barriers, potential security breaches, privacy concerns, transaction costs, and scalability issues. Equally significant is the evolving interplay between emerging technologies and shifting regulations. The rise of Central Bank Digital Currencies (CBDCs) signals profound changes in how nations perceive and engage with the broader crypto ecosystem. Navigating this terrain demands a nuanced approach that respects foundational principles while welcoming innovation.

In this dynamic landscape, CyberGold emerges not merely as a bystander but as a visionary navigator. CyberGold is acutely aware that the immutability of its foundational smart contracts offers both strength and inherent constraints. Yet, CyberGold views this as an invitation to innovate. Recognizing that technological advancements will inevitably usher in new challenges and opportunities, CyberGold understands that the final chapter in the evolution of stablecoins is still far away.

Final words

The numerous innovations found in the protocol underscore CyberGold's commitment to not only addressing present challenges but also shaping a brighter future in decentralized finance. As we stand at the threshold of this new era marked by collaboration, transparency, and innovation, the lessons from past pioneers of the crypto realm inspire us. Recognizing the strength in unity, we invite everyone who shares our vision to join the Cifero association. By pooling our collective knowledge and resources, we believe we can craft a more resilient, decentralized financial ecosystem, achieving collective milestones that might remain elusive if pursued in isolation.

Glossary

Arbitrage: The simultaneous purchase and sale of an asset in different markets to take advantage of differing prices for the same asset.

CBDC: Central Bank Digital Currency

Collateral: An asset that a borrower offers to a lender to secure a loan. If the borrower stops making the promised payments, the lender can seize the collateral to recoup its losses.

Convertibility: The quality that allows money or other financial instruments to be converted into other liquid stores of value.

Cypherpunk: An activist advocating widespread use of strong cryptography as a route to social and political change.

Decentralization: The process by which the activities of an organization, particularly those regarding decision-making, are distributed or delegated away from a central authority.

Ether (ETH): The native cryptocurrency of the Ethereum platform.

Exchange Rate Risk: The potential change in earnings due to a change in market exchange rates.

Front-running: The unethical practice of a broker trading an equity in his personal account based on advanced knowledge of pending orders from the brokerage firm or the clients, often seen in the context of oracle attacks in crypto.

Hedging: Making an investment to reduce the risk of adverse price movements in an asset.

Hedging Ratio: The proportion of an exposure or risk that is offset by a corresponding counter-position, often used to minimize potential losses from market fluctuations.

Liquid Staking: A method that allows cryptocurrency holders to earn rewards by participating in staking without locking up their assets.

Liquidity: The ease with which an asset, or security, can be converted into ready cash without affecting its market price.

Operational Modes (Standard, Recovery, Exit): The different states the CyberGold protocol can be in based on certain predefined conditions.

Oracle: A system that fetches real-world data to smart contracts on the blockchain.

Oracle Heartbeat: the maximum allowable delay between updates from an oracle.

Seigniorage: The profit made by a government by issuing currency, especially the difference between the face value of coins and their production costs.

Smart Contract: Self-executing contracts with the terms of the agreement directly written into lines of code.

Solvency: The ability of a company to meet its long-term financial obligations.

Stablecoin: A cryptocurrency that attempts to offer price stability by pegging its value to a reserve or basket of assets.

Third-party risk: The risk that comes from relying on external parties to provide a service or meet an obligation.

Vault (in the context of DeFi): A type of smart contract that users deposit funds into, often used in decentralized finance platforms.