Krypton: A Scalable, Privacy-Preserving, and Decentralized Search Engine for the Web3 Era

Akshat K. Parikh
Del Norte High School, San Diego, CA 92127, United States.

Email: akshat1228@gmail.com (A.K.P.)
Manuscript received August 30, 2023; accepted December 1, 2023; published December 15, 2023.
DOI: 10.18178/IJBTA.2023.1.2.95-112

Abstract: This paper presents an architectural overview and detailed design of the Krypton network, the first decentralized search engine built on Web3 principles. Krypton leverages blockchain technology, token-driven incentives, and privacy-focused features to revolutionize internet search. The proposed solution incorporates distributed storage, decentralized web crawling and indexing, a consensus mechanism, open-source search algorithms, and a privacy-focused search experience. Krypton introduces the novel concept of Proof of Learning, a machine learning protocol embedded in the search engine to facilitate the discovery of decentralized platforms and enable direct peer-to-peer networking. The system also employs decentralized cloud technologies (validators in the PoS blockchain) to promote enhanced decentralization and encryption, paving the way for a more secure and equitable internet.

Keywords: decentralization, search engines, blockchain, Web3

1. Introduction

The prevailing consensus in today's internet landscape is that data-driven platforms amass enormous profits and influence within the technology and retail sectors. The centralized nature of the internet will inevitably be challenged as decentralized networks with more advanced capabilities emerge. Web3 has long been envisioned as the successor to Web2 [1], offering greater privacy, security, and peer-to-peer interactions. Krypton is set to become one of the pioneering applications for Web3, serving as a platform and host akin to Google's role in the Web2 era. This innovative search engine will employ algorithms similar to those used by Google, while integrating the cutting-edge technology of blockchain to enhance its capabilities.

Inspired by *Ilya Zhitomirskiy*, co-founder of Diaspora, a decentralized social networking platform that prioritized user privacy and data ownership. Zhirtomirsky's vision of a decentralized internet, challenging the profit-driven model of traditional social media platforms, has inspired the development of decentralized technology projects like Krypton. Zhitomirskiy's legacy reminds us that technology can be a tool for promoting social justice and creating a more democratic and equitable world.

2. Krypton's Distributed Storage Framework

The main goal for Krypton is to be a completely privatized internet, meaning it follows the pattern of decentralization and gives sovereignty to the users, not the network.

2.1. IFPS and Filecoin

One of the key elements in building a decentralized search engine is implementing distributed storage systems for web pages and search indexes. Utilizing decentralized file storage systems, such as IPFS (InterPlanetary File System) or Filecoin, offers several advantages that contribute to the overall effectiveness and resilience of the search engine.

IPFS is a protocol and network designed to make the web faster, safer, and more open by replacing the

traditional centralized model of the web with a distributed, peer-to-peer network. In this system, each file and all of the blocks within it are given a unique fingerprint called a cryptographic hash. When looking up files on the network, users request them by their hashes, ensuring data integrity and reducing the reliance on a single server or data center (Fig. 1).

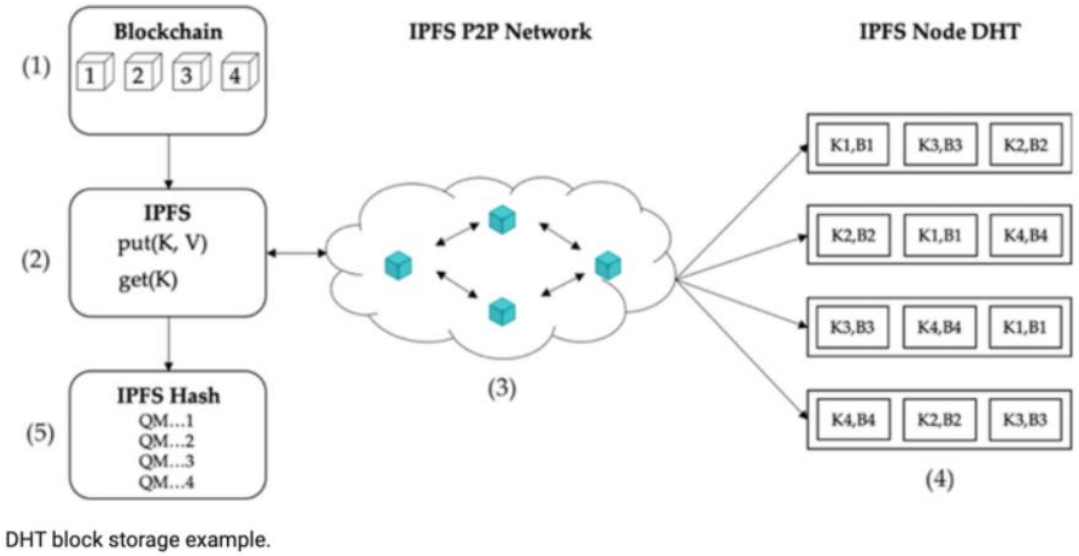

Fig. 1. DHT block storage example using IFPS P2P Network - Storage Gaga [2].

Filecoin, on the other hand, is a decentralized storage network built on top of IPFS that allows users to rent out their unused storage space in exchange for Filecoin tokens. This creates a competitive marketplace for storage, resulting in more efficient and cost-effective solutions.

By storing web pages and search indexes on distributed storage systems, the decentralized search engine can benefit from data redundancy, as multiple copies of the data are stored across the network. This redundancy ensures that the search engine remains operational even in the face of node failures or attempts to censor specific content.

2.2. Censorship

Censorship resistance is another crucial advantage of employing distributed storage in a decentralized search engine. Centralized search engines can be pressured or coerced into removing or de-ranking specific content, undermining the principle of an open and unbiased internet. In contrast, a decentralized search engine built on distributed storage systems is less susceptible to censorship due to its inherent redundancy and the absence of a single controlling authority.

By integrating Filecoin into Krypton's storage system, Krypton can benefit from a competitive storage marketplace, resulting in more efficient and cost-effective storage solutions. Additionally, Filecoin's native token (FIL) can be used to incentivize users to contribute their spare storage resources to the network, further strengthening the decentralized nature of Krypton's search engine.

Filecoin's content-addressed storage system ensures that data is securely and redundantly stored across multiple nodes in the network. As users contribute their storage resources, the network becomes more resilient to potential failures or censorship attempts. This approach aligns with Krypton's core principles of privacy, decentralization, and open access to information.

2.3. IFPS Incorporation

By incorporating IPFS into Krypton's storage system, the search engine can utilize its content-addressed, distributed storage model to maintain web pages and search indexes.

In IPFS, each file and its corresponding blocks are assigned a unique cryptographic hash, ensuring data integrity and enabling efficient content retrieval. Users can request files by their hashes, reducing the reliance on centralized servers or data centers [3], and promoting a more resilient and fault-tolerant network. Furthermore, IPFS's distributed nature contributes to Krypton's goals of censorship resistance and privacy

preservation.

Incorporating distributed storage systems like IPFS and Filecoin into a decentralized search engine is a vital component of the solution. This approach ensures data redundancy and censorship resistance while maintaining the integrity and availability of web pages and search indexes. The use of decentralized file storage systems contributes to creating a more resilient, equitable, and open web.

3. Decentralized Web Crawling & In Depth Indexing

Krypton's decentralized search engine aims to transform the way users access and interact with the internet by employing a decentralized web crawling and indexing system. This approach ensures that the search engine operates in a secure, efficient, and censorship-resistant manner. This section delves into the technical aspects of Krypton's decentralized web crawling and indexing, focusing on the creation of a network of nodes, the use of distributed hash tables (DHT), and incentivization through a native cryptocurrency or token.

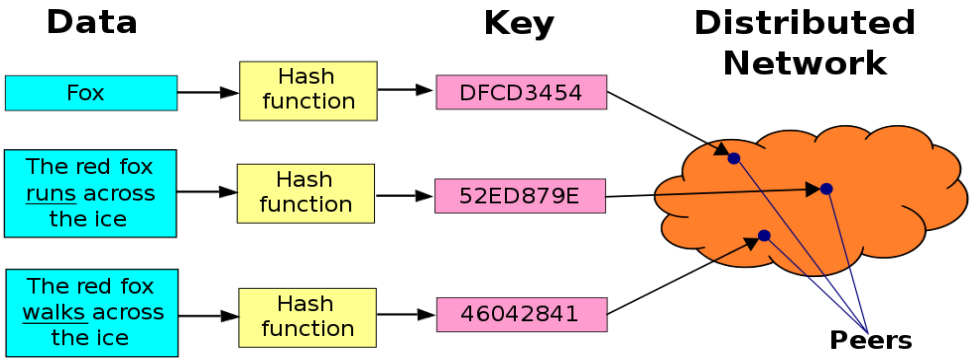

Fig. 2. Distributed hash tables - Wikipedia [4].

In Krypton's decentralized search engine, the process of web crawling and indexing is managed by a collaborative network of nodes that work in tandem to discover, catalog, and maintain web content. The technical aspects of this distributed approach help ensure that the workload is evenly balanced across the network, leading to reduced time and resource requirements for web crawling and indexing, ultimately enhancing the overall efficiency and responsiveness of the search engine.

Each node is assigned a specific subset of websites to crawl and index. This allocation is based on factors such as domain, content type, or geographical distribution. The partitioning of web content among nodes can be achieved through consistent hashing or other suitable partitioning techniques [Fig. 2). This division of labor ensures that no single node is overwhelmed by the task of crawling and indexing an excessively large portion of the web.

3.1. Peer-to-Peer Protocol Using DHTs

To facilitate seamless collaboration among nodes, Krypton employs a peer-to-peer communication protocol that enables nodes to exchange information about their assigned websites, newly discovered web pages, and index updates. This communication may involve the use of distributed hash tables (DHT) for efficient content discovery and routing, as well as a consensus mechanism to validate and synchronize index updates across the network. Specifically, Krypton employs a distributed hash table (DHT) for storing and retrieving index information. In this system, nodes store and share key-value pairs (cryptographic hash and associated content) for the content they index. The DHT enables nodes to quickly and efficiently locate and retrieve index data within the network, even as the number of nodes and indexed content increases.

3.2. Nodes Contributing Resources

Another solution would be to encourage nodes to contribute their resources (computing power, storage, and bandwidth) to the network, Krypton uses a native cryptocurrency or token as a reward mechanism. Nodes can earn these tokens by participating in web crawling and indexing activities, as well as by sharing their index data with other nodes in the network. This incentive structure ensures that the decentralized

search engine remains robust, secure, and self-sustaining, as nodes are motivated to continuously contribute their resources to maintain and improve the system.

3.3. Consensus Mechanisms

To ensure the accuracy and consistency of the indexed content across the network, Krypton implements a consensus mechanism for nodes to validate and agree on the data they share. This mechanism could be a variation of Proof of Work (PoW), Proof of Stake (PoS), or any other suitable consensus algorithm [5]. The consensus mechanism helps maintain the integrity of the indexed data, preventing potential attacks or manipulations that could compromise the search engine's performance and user experience.

3.4. Decentralized Web Crawling and Indexing

Decentralized web crawling and indexing play a crucial role in ensuring that Krypton remains resistant to censorship. By distributing the responsibility for indexing websites among multiple nodes, Krypton eliminates single points of failure or control. This approach makes it more difficult for external forces to influence or censor the search results, promoting an open, equitable, and accessible internet experience for users.

In addition, as the size of the web grows, Krypton's decentralized web crawling and indexing system is designed to scale accordingly. New nodes can be added to the network to accommodate increased web content, and the existing workload can be dynamically rebalanced among nodes to ensure optimal performance. Load balancing strategies, such as consistent hashing or rendezvous hashing, can be implemented to distribute the workload evenly across the network, minimizing bottlenecks and maximizing resource utilization.

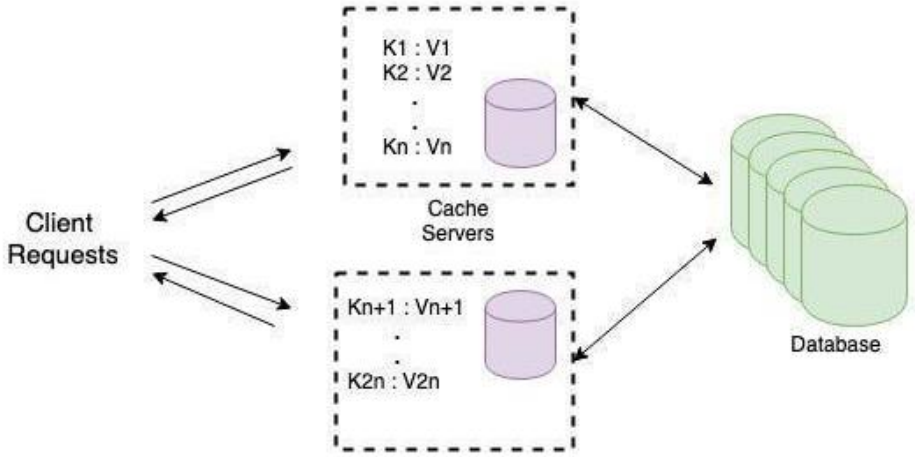

Fig. 3. Theorized off-chain based data storage mechanism - ResearchGate [5].

Krypton's decentralized approach to web crawling and indexing ensures fault tolerance by distributing the workload among multiple nodes. If a node fails or becomes unavailable, other nodes can detect this failure and take over its responsibilities, ensuring that web crawling and indexing operations continue uninterrupted. Additionally, index data can be replicated across multiple nodes, providing redundancy and further improving the system's resilience to node failures.

Krypton's decentralized search engine can also employ adaptive crawling and indexing strategies that enable nodes to dynamically adjust their behavior based on factors such as network conditions, content popularity, and resource availability. For instance, nodes can prioritize the crawling and indexing of frequently updated or high-traffic websites (Fig. 3), ensuring that the search engine remains up-to-date and responsive to user queries.

This proposed decentralized web crawling and indexing system employs a variety of technical components and strategies to ensure efficient, responsive, and scalable search engine performance. By distributing the workload among a network of nodes, Krypton is able to reduce the time and resources required for web crawling and indexing, creating a more resilient and efficient search engine for the decentralized web.

4. Consensus Mechanism, Ensuring Security & Accuracy

In Krypton's decentralized search engine, a robust consensus mechanism is crucial for maintaining the security and accuracy of search indexes and for preventing malicious behavior. A well-designed consensus mechanism ensures that nodes within the network can efficiently reach agreement on index updates, validate new content, and synchronize the distributed data. This section delves into the technical aspects of implementing a consensus mechanism, such as Proof-of-Stake (PoS), within Krypton's search engine infrastructure.

4.1. PoS

Proof-of-Stake (PoS) is a consensus algorithm in which nodes, referred to as validators, are chosen to create new blocks and confirm transactions based on the amount of cryptocurrency they hold (their stake) and other selection criteria. In Krypton's decentralized search engine, PoS can be adapted to ensure the security and accuracy of search indexes while reducing the energy consumption and resource requirements typically associated with Proof-of-Work (PoW) consensus mechanisms.

In the Krypton network, nodes that participate in the PoS consensus mechanism are known as validators. Validators are required to lock up (stake) a certain amount of the native cryptocurrency or token as collateral to ensure their commitment to maintaining the integrity of the search index. The staking mechanism helps create a financial disincentive for malicious behavior, as validators with malicious intent risk losing their staked tokens if they are caught attempting to manipulate the search index.

The PoS consensus mechanism involves a process in which validators are chosen to propose new blocks (index updates) and validate proposed changes to the search index. The selection of validators can be based on factors such as the amount of staked tokens, uptime, and past performance in maintaining the search index. Once a validator is chosen to propose a new block, other validators in the network are responsible for validating and confirming the proposed changes. A majority agreement among validators is required to finalize and commit the index update to the network.

For incentives and penalties regarding the network, validators that actively participate in the consensus process and contribute to maintaining the search index are rewarded with native cryptocurrency or tokens. These rewards serve as an incentive for validators to act honestly and diligently in their duties. Conversely, validators that engage in malicious behavior or fail to properly maintain the search index can face penalties, such as the forfeiture of their staked tokens or loss of future block rewards.

4.2. Implementing PoS for Krypton

Implementing a PoS consensus mechanism in Krypton's decentralized search engine helps to enhance the security of the search index and protect against potential attacks. The staking requirement and validator selection process make it more difficult for malicious actors to gain control of the network or manipulate the search index [5], as acquiring a majority stake in the network would be both costly and risky.

The integration of a consensus mechanism, such as Proof-of-Stake, within Krypton's decentralized search engine plays a vital role in maintaining the security, accuracy, and integrity of the search indexes. By leveraging the benefits of PoS, Krypton can efficiently prevent malicious behavior, ensure a fair and transparent search engine, and promote a more sustainable and energy-efficient approach to consensus in the decentralized web.

5. Search Algorithms & Ranking: A Transparent Approach

One of the critical components of Krypton's decentralized search engine is the development and implementation of search algorithms and ranking systems that are transparent, customizable, and community-driven. By adopting this approach, Krypton aims to deliver unbiased search results and promote a more diverse range of content, setting itself apart from traditional, centralized search engines. In this section, we delve into the technical aspects and benefits of Krypton's search algorithms and ranking systems.

5.1. Open-Source Model

By adopting an open-source model for its search algorithms, Krypton ensures complete transparency, enabling users, developers, and researchers to scrutinize and understand the underlying mechanisms that drive search results. This level of transparency promotes accountability and prevents potential manipulation or biases within search results.

Open-source search algorithms facilitate contributions from the community, allowing developers and

researchers to propose enhancements, optimizations, and novel techniques. This collaborative environment fosters ongoing improvement and innovation, ensuring Krypton's search engine remains at the forefront of search technology.

5.2. Customizing Search Algorithms

To enhance the user experience and further minimize the influence of any single entity, Krypton enables users and developers to customize the search algorithms. This feature allows individuals to adjust parameters, filter content, and even create their own ranking criteria based on their needs and preferences. As a result, Krypton offers a search experience that truly caters to individual users while reducing the risk of centralized biases.

5.3. Decentralized Ranking System

In parallel with the open-source and customizable search algorithms, Krypton implements a decentralized ranking system. This system takes into account various factors such as user feedback, domain authority, and content relevance. By distributing the ranking process across a network of nodes, Krypton diminishes the likelihood of centralization and undue influence that could lead to biased search results. Furthermore, this decentralized approach empowers users to directly impact search result rankings through their interactions and feedback [5].

User feedback is an essential component of Krypton's ranking system. By incorporating user feedback, Krypton can ensure that the search results align with the preferences and interests of its users. The technical implementation of user feedback involves users assigning ratings or rankings to search results, flagging spam or inappropriate content, or providing comments on the relevance or quality of the content [6].

5.4. End-to-End Encryption (Will Be Discussed more in Depth Later on)

Krypton will also employ end-to-end encryption to ensure that user feedback is secure and private. The encrypted feedback data is then transmitted to the responsible node in the network, which processes and aggregates the feedback along with feedback from other users. This aggregated information is then used to update the ranking of the search results and improve the search algorithm.

5.5. Domain Authority, Nodes, DHTS, and Content Relevance

Domain authority is a metric used to assess the credibility and quality of a website based on factors such as the number of inbound links, the quality of those links, and the site's age. In Krypton's decentralized search engine, domain authority is calculated by each node in the network for the websites it is responsible for indexing.

Nodes employ a distributed hash table (DHT) to share and exchange domain authority information with other nodes in the network. The domain authority data, combined with other ranking factors, is used to adjust the position of websites in the search results [7]. This helps ensure that search results prioritize trustworthy and reputable websites, contributing to the overall quality of the search experience.

Content relevance is another crucial factor in Krypton's ranking system, as it ensures that search results are closely related to the user's query. To assess content relevance, Krypton's search algorithms employ natural language processing (NLP) techniques and semantic analysis to evaluate the similarity between the user's query and the content of indexed web pages.

Each node in Krypton's network is responsible for evaluating content relevance for its assigned subset of websites. The node analyzes the web pages and assigns a relevance score based on factors such as keyword frequency, keyword proximity, and semantic context. These relevance scores are then shared and exchanged with other nodes using the DHT, allowing Krypton's search engine to rank the search results based on their relevance to the user's query.

Krypton also incorporates incentive mechanisms to promote high-quality, relevant, and trustworthy content. By linking rewards to factors like user feedback, domain authority, and content relevance, Krypton encourages content creators and website owners to prioritize valuable content. This strategy helps to discourage spam or low-quality websites from dominating search results, leading to a more diverse and unbiased range of content.

5.6. Conclusion

In essence, all of these components work together harmoniously in Krypton's decentralized search engine. The open-source search algorithms, customizable and community-driven development, decentralized ranking system, and incentive mechanisms for quality content form an interconnected system that ensures transparency and prevents bias within search results. By integrating these elements, Krypton creates a fair, equitable, and user-centric internet experience that prioritizes the needs and preferences of its users.

6. Privacy & End-to-end Encryption Models

One of the key differentiators of Krypton's decentralized search engine, in addition to its transparent and unbiased search results, is its strong commitment to user privacy. In this segment, we explore the privacy-focused search experience provided by Krypton, discussing the implementation of end-to-end encryption, zero-knowledge proofs [8], and other privacy-enhancing techniques that protect user data and search queries from third parties.

Krypton's search engine will employ end-to-end encryption, a powerful privacy-enhancing technique that ensures the confidentiality of user data and search queries. End-to-end encryption works by encrypting data on the user's device before transmission, such that only the intended recipient can decrypt and access the information. In the context of Krypton's search engine, this means that search queries and user data are encrypted on the user's device, rendering them unreadable to any intermediaries, including Krypton's network nodes or potential adversaries.

By incorporating end-to-end encryption into its search engine, Krypton significantly enhances user privacy and security. Users can confidently perform searches without fear of their queries or personal data being intercepted, analyzed, or exploited by third parties. This protection extends to the user's browsing history and preferences, ensuring that Krypton's search engine remains a safe and private space for users to explore the web.

6.1. Paillier Cryptosystem

The Krypton network will use several end to end encryption models, with the primary encryption model being a “Paillier Cryptosystem”. The Paillier Cryptosystem, named after its creator *Pascal Paillier*, is a public-key cryptosystem with unique homomorphic properties. It enables the performance of specific computations on encrypted data without the need to decrypt it first, providing valuable privacy-preserving benefits [9] for Krypton's decentralized search engine.

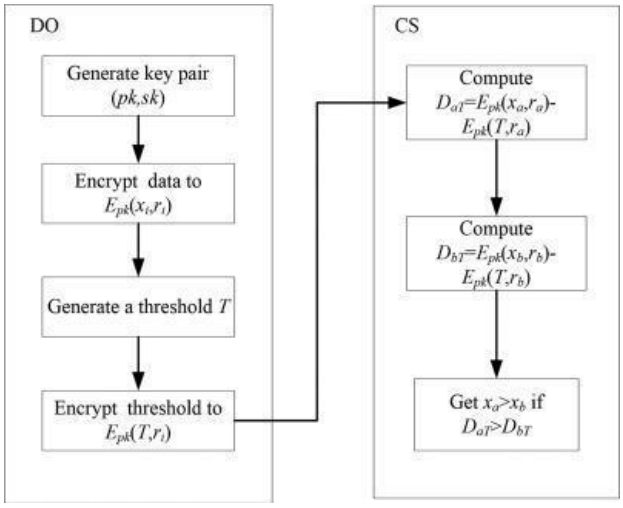

Fig. 4. Pascal paillier cryptosystem - ScienceDirect [9].

In the context of the Paillier Cryptosystem, homomorphic encryption refers to the ability to perform specific mathematical operations on ciphertext (encrypted data) while preserving the relationship between the plaintext (unencrypted data) and the results. The Paillier Cryptosystem is additively homomorphic (Fig. 4), meaning that it allows for the addition of plaintext values by performing operations on their corresponding ciphertexts.

Krypton can utilize the Paillier Cryptosystem to process user feedback, such as ratings or rankings, in an encrypted form. By performing necessary computations on encrypted feedback data, Krypton can aggregate

and analyze user input without compromising user privacy. This approach ensures that sensitive user information remains secure, even when processed by the nodes in the network.

Krypton can employ the Paillier Cryptosystem to process search queries securely. When users submit search queries, the queries are encrypted using the Paillier Cryptosystem, and nodes can perform computations on the encrypted queries to generate search results. This method preserves user privacy, as the search queries remain encrypted throughout the entire process.

The Paillier Cryptosystem's homomorphic properties can also be leveraged for privacy-preserving analytics within the Krypton network. Encrypted user data, such as search patterns and user preferences, can be analyzed to improve the search engine's performance and enhance the user experience. By processing the encrypted data, Krypton can gain valuable insights without exposing sensitive user information.

Integrating the Paillier Cryptosystem into Krypton's decentralized search engine would require adapting the cryptosystem to the network's specific requirements and architecture. Key considerations include key management, secure communication between nodes, and efficient computation on encrypted data.

Developers would need to devise a system for generating and distributing public and private key pairs to users and nodes within the network. Additionally, the implementation should ensure that encrypted data is securely transmitted between users and nodes, as well as among nodes when sharing information.

By implementing the Paillier Cryptosystem, Krypton can offer a privacy-focused search experience that respects user data confidentiality and enables secure processing of sensitive information throughout the network. This approach aligns with Krypton's commitment to providing a secure, decentralized Web3 search engine that prioritizes user privacy and data protection.

6.2. Noise Protocol Framework (NFP) & Advantages of Utilizing NFP

Krypton can certainly implement the noise protocol framework as well, a flexible and modular framework for building secure end-to-end encryption protocols. It is used in secure communication systems such as the WireGuard VPN and the Lightning Network. By employing the Noise Protocol Framework, Krypton can design custom end-to-end encryption protocols that fit the specific requirements of its decentralized search engine. This approach allows for optimized performance and security tailored to Krypton's unique architecture.

The Noise Protocol Framework consists of several core components, one of them being handshake patterns. Handshake patterns define the sequence of messages exchanged between parties to establish a secure communication channel [10]. The framework offers a variety of predefined handshake patterns, which can be customized to suit Krypton's specific needs.

The framework supports a range of cryptographic primitives, including encryption schemes, key derivation functions, and digital signature algorithms. Krypton can choose from these primitives based on its security requirements and performance needs.

The Noise Protocol Framework also allows for the composition of multiple protocols, enabling the development of modular and layered encryption systems. This composability ensures that Krypton can easily extend or modify its encryption protocols as needed.

Implementing the Noise Protocol Framework in Krypton's decentralized search engine offers several advantages:

- Krypton can design custom end-to-end encryption protocols that cater to the specific requirements of its decentralized search engine. This flexibility enables Krypton to optimize performance and security based on its network architecture, user privacy needs, and other factors.
- The Noise Protocol Framework's modular design allows Krypton to scale its encryption protocols as the network grows. By incorporating new cryptographic primitives or modifying handshake patterns, Krypton can ensure that its encryption protocols remain secure and efficient.
- The Noise Protocol Framework [10] is designed for compatibility and can be easily integrated with other cryptographic systems and protocols. This interoperability enables Krypton to leverage existing security technologies and establish secure communication channels with other Web3 services and platforms.

6.3. Implementation

To implement this protocol we would need to analyze Krypton's specific security requirements, performance needs, and architectural constraints to determine the most suitable handshake patterns, cryptographic primitives, and protocol configurations.

We would also need to establish secure communication channels between users and nodes within Krypton's network, ensuring that search queries, user feedback, and other sensitive data are securely transmitted and processed.

6.4. Conclusion

By employing the Paillier Cryptosystem and Noise Protocol Framework, Krypton can develop tailored end-to-end encryption protocols that address its unique security challenges and provide a robust, privacy-preserving search experience for users. This approach aligns with Krypton's commitment to building a secure, decentralized Web3 search engine that prioritizes user privacy and data protection.

7. Privacy with Zero-knowledge Proofs, SMPC, Homomorphics

Another privacy-enhancing technique employed by Krypton is the use of zero-knowledge proofs. Zero-knowledge proofs enable one party to prove the validity of a statement without revealing any information about the statement itself. In the context of Krypton's search engine, this could be applied to verify user actions or transactions without exposing the details of the actions or transactions themselves.

7.1. Integration of Zero-Knowledge Proofs

By integrating zero-knowledge proofs into its search engine, Krypton can provide a greater level of privacy for its users. For example, Krypton could use zero-knowledge proofs to verify the authenticity of user rankings or feedback without disclosing the identity of the users who submitted them. This approach further reinforces the privacy-focused search experience, allowing users to contribute to the search engine's development while maintaining their anonymity.

The incorporation of end-to-end encryption and zero-knowledge proofs in Krypton's decentralized search engine aligns with the core principles of Web3. Web3 envisions an internet that is more private, secure, and peer-to-peer, with users having greater control over their data and online experiences. By implementing privacy-enhancing techniques, Krypton's search engine exemplifies these values, offering users a search experience that prioritizes their privacy and security.

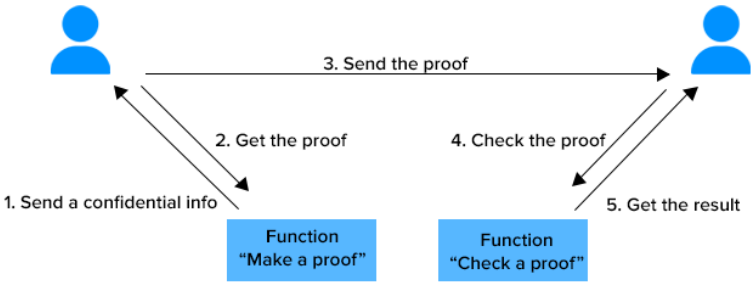

Fig. 5. Sample mechanism of zero-knowledge proofs - ECrypto News [11]

Krypton's decentralized search engine embraces privacy-focused features such as end-to-end encryption and zero-knowledge proofs to protect user data and search queries from third parties. These privacy-enhancing techniques contribute to the overall vision of a Web3 search engine that is private, secure, and user-centric, setting Krypton apart from traditional, centralized search engines and laying the foundation for a more equitable and user-oriented internet experience.

In addition to zero-knowledge proofs, there are other privacy-enhancing technologies that Krypton could consider implementing to ensure user privacy and data protection. Some of these solutions include Secure Multi-Party Computation (SMPC) and Homomorphic Encryption.

7.2. Potential Integration of SMP Computation

Secure Multi-Party Computation (SMPC) is a cryptographic technique that enables multiple parties to collaboratively compute a function over their respective inputs while keeping those inputs private. In the context of the Krypton network, SMPC could be employed to process user feedback or search queries without exposing the user's data to other nodes (Fig. 5). By leveraging SMPC, Krypton would be able to perform necessary computations and generate accurate search results without jeopardizing user privacy.

7.3. Homomorphic Encryption & Conclusion

Another privacy-enhancing solution is Homomorphic Encryption, a form of encryption that allows specific computations to be performed on encrypted data without requiring decryption. This technology could be particularly useful for Krypton when processing user feedback, search queries, or other sensitive information. By implementing Homomorphic Encryption, Krypton can ensure that user data remains encrypted and secure while still allowing for the necessary processing and analysis to generate meaningful search results.

Both SMPC and Homomorphic Encryption can complement zero-knowledge proofs in Krypton's efforts to create a privacy-focused search experience. These technologies, when combined with a robust and secure underlying network infrastructure [12], would help Krypton build a decentralized search engine that prioritizes user privacy and data protection. By incorporating these privacy-enhancing solutions, Krypton can foster trust among its users and differentiate itself from traditional, centralized search engines that often rely on the collection and monetization of user data.

8. A Token-Based System for User Engagement and Network Growth

The Krypton Incentive Model revolves around the creation of a native utility token, KRPT, which serves as the primary means of rewarding users for their contributions to the network. Users can earn KRPT tokens by participating in any of the following activities:

- Validating Transactions
- Providing Resources
- Giving Feedback on Search Results

8.1. Validating transactions

As a decentralized platform, Krypton relies on its users to validate transactions and maintain the integrity of the network. Users who stake their KRPT tokens and act as validators are rewarded with a portion of the transaction fees collected, in addition to newly minted KRPT tokens.

8.2. Providing resources

Users can contribute to Krypton's decentralized infrastructure by offering storage, bandwidth, or computational resources. In return, they receive KRPT tokens proportional to the resources they provide. This incentivizes users to support the network, ensuring its scalability and sustainability.

8.3. Giving Feedback

To enhance the quality of search results within the Krypton ecosystem, users can submit feedback on the accuracy and relevance of search outputs. By doing so, they help to improve the platform's algorithms, benefiting the entire Krypton community. Users who provide valuable feedback will be rewarded with KRPT tokens.

8.4. KRPT Supply

The total supply of KRPT tokens is fixed, with a portion allocated to the Krypton Foundation for platform development and marketing efforts. The remaining tokens are distributed to users through the activities mentioned above. Additionally, KRPT token holders have a say in the platform's governance, allowing them to vote on proposals and influence the future direction of the network.

8.5. Search Engine Rewards

The Krypton search engine plays a pivotal role in providing users with high-quality and relevant search results. To further incentivize user engagement, KRPT tokens are awarded to users based on their search activity. Users can earn tokens by actively using the search engine, making it their default search provider, and sharing it with friends and family. This approach not only rewards users for their search activities but also helps drive user growth and adoption of the Krypton platform.

8.6. Staking Rewards

Staking is another crucial aspect of the Krypton Incentive Model. Users can lock their KRPT tokens in a staking contract for a predetermined period, during which they support network security and earn a portion of the block rewards. The staking rewards are determined by the amount of KRPT staked, the duration of the staking period, and the overall network participation rate. Staking not only provides users with a passive income stream but also secures the Krypton network by encouraging the holding of KRPT tokens.

8.7. Yield-Farming & Lending Opportunities

Krypton will also implement yield farming opportunities within its search for users interested in earning passive income from their KRPT holdings. Users can stake their tokens in liquidity pools or lending platforms, enabling others to borrow or trade against their staked assets. In return, users receive a share of the platform's fees, such as trading or borrowing fees, as well as additional KRPT tokens. This mechanism encourages users to hold and use their tokens, promoting long-term growth and stability of the Krypton ecosystem.

8.8. Reward System Conclusion

This incentive model offers a robust and sustainable mechanism to reward users for their contributions to the network. By implementing this token-based system, Krypton aims to build a thriving and self-sustaining ecosystem, where users are motivated to actively engage in the network's growth and optimization.

9. Strategies to Strengthen the KRPT Reward System

An important matter is to ensure that KRPT’s incentive model stays intact and doesn’t end up disrupting the Krypton network.

9.1. Tiered Reward System for Krypton Users

One way is to introduce a tiered incentive structure that can help ensure the Krypton reward system remains effective and engaging. Users can achieve different levels based on their accumulated KRPT tokens or contribution to the platform. Each level grants users access to additional benefits and higher reward rates, motivating them to continue contributing to the network and holding KRPT tokens.

9.2. KRPTRS - Krypton Reputation Reputation System

Implementing a reputation system can also help improve the quality of user contributions and promote healthy competition among participants. Users earn reputation points for their validated contributions, such as providing accurate feedback on search results or successfully validating transactions. A higher reputation score translates to better rewards and additional privileges within the Krypton ecosystem. This system encourages users to maintain a high level of engagement and strive for excellence.

9.3. Token Burns and Buybacks

Token burns and buybacks are mechanisms that can be employed to regulate the circulating supply of KRPT tokens, thereby ensuring the token's value remains stable (Fig. 6). Periodic token burns can be implemented, where a portion of the collected platform fees is used to permanently remove a specific amount of KRPT tokens from circulation. Buybacks involve using a portion of the platform's revenue to purchase KRPT tokens from the open market and redistribute them as rewards or burn them. These strategies can help maintain a healthy token economy and encourage user participation.

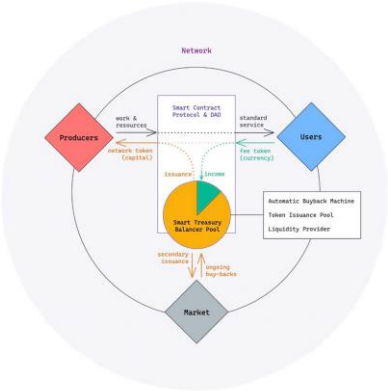

Fig. 6. Token burns and buyback mechanism - Placeholder VC [13].

10. Establishing Partnerships to Create the Krypton Network

Establishing partnerships with other platforms and organizations can increase the utility and value of KRPT tokens, further incentivizing users to engage with the Krypton ecosystem. Collaborative initiatives can include integrating KRPT as a payment option on partner platforms, cross-chain collaborations, or offering exclusive promotions and discounts to KRPT holders. These partnerships not only broaden the use cases for KRPT tokens but also attract new users to the Krypton platform.

One partnership that heavily increases the utility and value of KRPT would be to partner with the COSMOS blockchain. Collaborating with COSMOS [14] would enable Krypton to tap into a larger ecosystem of interconnected blockchains, potentially increasing the utility and value of KRPT tokens.

What can Krypton offer within its network? Here is what potential partnerships can amount to for the Krypton network:

- Partnering with DeFi platforms like Aave or Compound can also enable KRPT holders to access various financial services such as lending, borrowing, and staking, further increasing the token's utility and value.
- By collaborating with NFT marketplaces such as OpenSea or Rarible, Krypton can integrate KRPT as a payment option for buying and selling digital assets. This partnership would enhance the token's use cases and attract new users interested in the NFT space.
- Partnering with DEXs like Uniswap or SushiSwap can enable seamless trading of KRPT tokens against other cryptocurrencies, improving liquidity and market access [8] for KRPT holders. Users can also trade other currencies and improve their liquidity as well.
- Krypton will collaborate with e-commerce platforms (Origin Protocol, OpenBazaar, etc.), allowing KRPT to be used as a payment method for online purchases. This partnership can boost the token's adoption and utility.
- Krypton can implement decentralized social media and video streaming platforms (Steemit, Theta Network, DLive, Mind, etc.) with no centralization, no advertising, all of it controlled by various DAOs and the KRPT decentralized ecosystem.
- Krypton can also establish partnerships with blockchain-based gaming platforms (Decentraland, The Sandbox, etc.), enabling the use of KRPT tokens for in-game purchases, rewards, or as a cross-platform currency. This collaboration can attract users from the gaming community to the Krypton ecosystem.
- Implementing and partnering with data storage platforms (Filecoin, Storj, etc.) can also help Krypton be a network that allows users to rent out their excess storage space and earn FIL tokens or Storj rewards in return, all under the one network [10] of Krypton.
- A decentralized prediction market platform built on blockchains (Augur, Gnosis, etc.) will allow Krypton users to create and participate in prediction markets/events using cryptocurrencies

10.1. Additional Features Theorized within the Krypton Network

- Krypton can implement a decentralized identity management system that allows users to have secure and private control over their personal data. This system would enable users to selectively share their information with third parties while maintaining privacy and security.
- Krypton encourages the creation and management of DAOs, allowing users to form decentralized

communities with shared goals and decision-making processes. This feature would empower users to collaborate on various projects and initiatives within the Krypton ecosystem. Remember, the Krypton network has no power, only its community does.

- Krypton can integrate a decentralized VPN service that provides users with increased privacy and security when accessing the internet. This feature would enable users to protect their online activity and bypass geographic restrictions while using the Krypton platform.
- We leave it to DAOs to destroy potentially harmful communities in exchange for KRPT rewards.
- Krypton can create a decentralized knowledge sharing platform that allows users to contribute and access educational content. Users can earn KRPT tokens for creating high-quality content or participating in courses, promoting lifelong learning and skill development within the Krypton community.
- The use of smart contracts can play an immense role in the Krypton ecosystem. Krypton can facilitate the creation of decentralized insurance products that leverage smart contracts and blockchain technology to provide transparent, efficient, and secure coverage. This feature would allow users to access insurance services without relying on traditional intermediaries.
- Krypton can develop solutions that enable seamless integration of Internet of Things (IoT) devices within its ecosystem [13]. This would allow users to manage and interact with their IoT devices using Krypton's platform and KRPT tokens
- Krypton can introduce a decentralized crowdfunding platform that enables users to raise funds for various projects and initiatives using KRPT tokens. This feature would promote innovation and help bring new ideas to life within the Krypton community.

10.1.1. Conclusion

For each service, DAOs or individuals will propose a new solution to be added within the Krypton network. We expect other users or DAOs to research and analyze the proposed solution in order to understand the requirements, potential challenges, and the benefits this new solution/feature will bring to the Krypton ecosystem. There are no restrictions within the Krypton network; anyone can incorporate any decentralized functionality or blockchain technology as desired.

11. Krypton's Governance Model

Krypton's governance model aims to create a decentralized decision-making process that ensures the platform remains community-driven and adapts to the evolving needs and preferences of its users. This model will emphasize the role of KRPT token holders, enabling them to actively participate in the decision-making process and shape the future development of the Krypton ecosystem.

11.1. Governance Model

The Krypton governance system will be built around the use of KRPT tokens. KRPT token holders will have the ability to propose changes, vote on proposals, and influence the platform's development. The weight of a user's vote will be determined by the number of KRPT tokens they hold, ensuring that those with a larger stake in the ecosystem have a more significant impact on decision-making.

11.2. Proposals

Any KRPT token holder can submit proposals for changes or improvements to the Krypton platform. These proposals can include, but are not limited to, adjustments to the reward system, new platform features, changes to the consensus mechanism, or updates to the token economy. To submit a proposal, users will be required to lock a predetermined amount of KRPT tokens as a commitment to the proposal's success. This ensures that only serious proposals are submitted for consideration.

11.3. Voting

Krypton will implement a transparent and fair voting mechanism to enable community involvement in decision-making processes. Once a proposal is submitted, it will enter a voting period during which KRPT token holders can cast their votes. The weight of each vote will be proportional to the number of KRPT tokens held by the voter. This ensures that the community's collective interests are represented in the final decision.

To pass a proposal, a minimum quota (e.g 2.5% of the total KRPT token supply) must participate in the voting process, and a predetermined majority must vote in favor of the proposal. If the required quota or

majority is not reached, the proposal will be considered rejected.

11.4. Successful Proposals

Once a proposal has been approved by the community, the proposed changes will be implemented by DAOs and blockchain developers who are a part of the Krypton network, in a timely and efficient manner. Regular updates on the progress of the implementation will be provided to the community to ensure transparency and maintain accountability.

11.5. Delegation

To encourage broader participation in the governance process, Krypton will support delegated voting. This feature allows KRPT token holders who may not have the time, knowledge, or inclination to participate in the voting process to delegate their voting power to a trusted community member or expert. Delegated voting ensures that the interests of all KRPT token holders are represented in the decision-making process, even if they cannot actively participate.

11.6. Governance Conclusion

Krypton's governance model, centered around KRPT token holders, ensures that the platform remains community-driven and responsive to the needs of its users. By enabling users to propose changes, vote on proposals, and participate in the platform's decision-making processes, Krypton fosters an inclusive and collaborative ecosystem that empowers its community to shape the platform's future.

12. Scalability & Preserving Infrastructure

The primary scalability challenges that Krypton may face include an increasing number of transactions, growing storage requirements, and the need for efficient query processing. These factors can impact the platform's responsiveness, speed, and overall user experience if not adequately addressed.

To address scalability challenges, Krypton will employ a layered architecture that separates the platform's core components into distinct layers. This approach allows for the independent scaling of each layer, ensuring that the platform can adapt to growing demands without compromising performance.

12.1. Krypton Sharding

The network will implement sharding, a technique that divides the network into smaller, more manageable segments called shards. Each shard will handle a portion of the platform's transactions and storage requirements, enabling parallel processing and improving the overall throughput of the system [12]. As Krypton grows, additional shards can be added to accommodate increased demand.

- The network will be divided into multiple shards, each shard is responsible for handling a sp-ecific portion of the platform’s transactions and storage.
- Each shard has its own set of validators which validate transactions and maintain the shard’s ledger
- Validators will be assigned to specific shard, assignment is completely random, no authority decides this
- When users interact with Krypton's platform, their transactions will be routed to the appropriate shard based on a predetermined sharding algorithm.
- Since each shard processes transactions independently and in parallel, the overall throughput of the Krypton network is significantly improved, as it can handle more transactions simultaneously compared to a non-sharded network.

12.2. Off-Chain Solutions & Caching/Indexing

Krypton will explore the use of off-chain solutions to improve scalability. Off-chain solutions, such as state channels and sidechains, enable the platform to process transactions and store data outside the primary blockchain, reducing the burden on the main network. This approach can help maintain high performance and responsiveness, even as usage increases (Fig. 7).

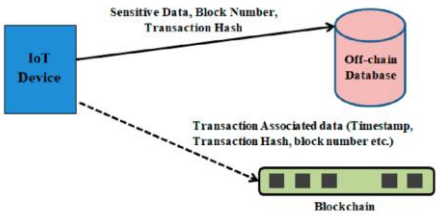

Fig. 7. Original theorized off-chain based data storage mechanism - ResearchGate [10].

Krypton will employ caching and indexing techniques to optimize the performance of its search engine. By caching frequently accessed data and maintaining efficient indexes, Krypton can quickly process user queries and deliver relevant search results with minimal latency.

12.3. Layer 2 solution

The network will also ensure its platform is compatible with Layer 2 scaling solutions, such as Plasma, zkRollups, and Optimistic Rollups. These solutions can help improve transaction throughput and reduce latency, enabling Krypton to accommodate more web3 products and protocols without compromising performance.

12.4. Monitoring and Optimization

Krypton will actively monitor its platform's performance and scalability, identifying and addressing bottlenecks and inefficiencies as they arise. This continuous optimization process will ensure that Krypton remains agile and responsive to the evolving needs of its users and the web3 ecosystem.

12.5. Scalability & Preserving Infrastructure Conclusion

By employing a combination of architectural design, sharding, off-chain solutions, caching, indexing, and interoperability with Layer 2 solutions, Krypton can effectively address scalability challenges and maintain its platform's performance as it grows. This proactive approach to scalability ensures that Krypton can continue to accommodate more web3 products and protocols, providing a seamless and efficient user experience even as usage increases.

13. Interoperability

Interoperability is a critical aspect of Krypton's vision to create a comprehensive search engine and network that hosts a wide range of web3 products and protocols. By ensuring seamless interoperability, Krypton can provide users with a unified experience across various blockchain ecosystems, simplifying access to decentralized applications and resources.

13.1. Cross-Chain Communication

Krypton will implement cross-chain communication solutions to enable the smooth interaction between different blockchain networks. These solutions will allow Krypton to facilitate the transfer of information, assets, and tokens between various blockchains, ensuring a cohesive experience for users. A potential cross-chain communication technology that Krypton may adopt is Comos Network's Interchain Communication Protocol (ICP). The ICP Protocol is a protocol that enables the exchange of data and tokens between blockchains within the Cosmos ecosystem [14].

Implementing Polkadot's Substrate framework is also another option as its modular framework allows for seamless communication between different blockchains.

13.2. Data-Sharing and Bridging Protocols

As mentioned earlier, Krypton will employ decentralized storage solutions, such as the InterPlanetary File System (IPFS) or Filecoin, to facilitate data sharing among various web3 products and protocols. By leveraging these decentralized storage solutions, Krypton can ensure that shared data remains secure, tamper-proof, and accessible across different blockchain networks.

Krypton will integrate bridging protocols that enable the transfer of assets and tokens across different blockchain networks. These bridging protocols allow users to easily move their assets between various web3 products and protocols without the need for complex, manual processes.

Two bridging protocols that Krypton may adopt is ChainBridge or RenVM. Chainbridge is a multi-directional blockchain bridge that supports various networks and enables the transfer of tokens and data between them. RenVM on the other hand, is an open protocol that provides access to inter-blockchain liquidity for decentralized apps, allowing the movement of assets between blockchains.

13.3. Integration/Token Standards

Krypton will support interoperable standards, such as ERC-20, ERC-721, and ERC-1155 token standards, to ensure compatibility with various web3 products and protocols. By adhering to widely-accepted token standards, Krypton can provide a seamless experience for users interacting with different decentralized applications and assets.

13.4. Interoperability Conclusion

By focusing on cross-chain communication, data sharing, bridging protocols, and token standards, Krypton aims to provide a seamless and interconnected experience for users across various web3 products and protocols. This interoperability ensures that Krypton can deliver a unified platform that simplifies access to decentralized applications and resources while fostering a collaborative and interconnected web3 ecosystem.

14. Proposal Conclusion

Krypton proposes a solution that unifies the diverse landscape of web3 products and protocols under a single, cohesive platform. By addressing key aspects such as distributed storage frameworks, web crawling and indexing, consensus mechanisms, search algorithms, decentralized ranking, end-to-end encryption, zero-knowledge proofs, secure multiparty computation, token-based systems, network growth strategies, and partnerships with other decentralized products, Krypton creates a robust and comprehensive ecosystem that fosters innovation and collaboration.

At its core, Krypton's governance model ensures that the platform remains community-driven and adaptable, empowering users to actively participate in decision-making processes and shape the future development of the ecosystem. The focus on scalability and interoperability also allows Krypton to easily accommodate a growing number of web3 products and protocols], providing users with a unified and interconnected experience.

Through the proposed integration of solutions such as sharding, off-chain solutions, caching, and indexing, Krypton effectively addresses potential scalability challenges, ensuring optimal performance and responsiveness even as usage increases. Furthermore, Krypton proposes solutions for cross-chain communication, data sharing, and bridging protocols which establishes a versatile platform that simplifies access to decentralized applications and resources across various blockchain networks.

Krypton's platform will host a diverse range of web3 features and services, including decentralized social media platforms like Steemit, video streaming services such as Theta, virtual reality platforms like Decentraland, and decentralized financial services like Aave. By supporting the integration of these and many other dApps, Krypton becomes a one-stop destination for users to access the decentralized web.

In conclusion, Krypton serves as a powerful solution that brings together the best of the web3 ecosystem under one network. By combining advanced technologies, innovative features, and a strong focus on community involvement, Krypton paves the way for a more connected, efficient, and accessible decentralized future.

Appendix

- WEB 3: Web 3.0, a concept for computing that pictures a new generation for internet networks and computing
- Proof of Learning: A system where a model owner logs training checkpoints to establish a proof of having expended the computation necessary for training.
- PoS: Proof-of-stake protocols are a class of consensus mechanisms for blockchains that work by selecting validators in proportion to their quantity of holdings in the associated cryptocurrency.

- IFPS: The InterPlanetary File System is a protocol, hypermedia and file sharing peer-to-peer network for storing and sharing data in a distributed file system.
- Filecoin: Filecoin is an open-source, public cryptocurrency and digital payment system.
- DHT: Distributed Hash Tables, nodes can be added or removed for re-distributing keys
- Validator: A participant in a Proof of Stake (PoS) blockchain network that is responsible for validating new transactions and maintaining the security of the blockchain.
- Paillier Cryptosystem: A probabilistic asymmetric algorithm for public key cryptography.
- Noise Protocol Frameworks: The Noise protocol framework is a suite of channel establishment protocols, ensures security properties
- Zero-Knowledge Proofs: A zero-knowledge protocol is a method by which one party can prove to another party that something is true, without revealing any information
- SMPC: Secure multi-party computation is a subfield of cryptography with the goal of creating methods for parties to jointly compute a function over their inputs while keeping those inputs private
- Homomorphism (Computing): The conversion of data into ciphertext that can be analyzed and worked with as if it were still in its original form
- KRPT: The Krypton Token
- Yield Farming and Token Burns: A way to earn rewards by depositing your cryptocurrency. Token burns remove coins from circulation, permanently decreasing the overall supply of the cryptocurrency.
- DAO: A decentralized autonomous organization, is an organization managed in whole or in part by decentralized computer program
- Sharding (Computing): Sharding is a process that divides the whole network of a blockchain organization into several smaller networks
- IoT: Internet of Things, a network of physical objects—“things”—that are embedded with sensors, software, and other technologies
- dApp(s) - Deentraland, Polkadot, The SandBox, Storj, Angur, Gnosis, Aave, COSMOS, Uniswap, Sushiswap, etc.
- DeFi: Decentralized Finance
- Bridging Protocols: ChainBridge and RenVM
- Interoperable Standards: ERC-20, ERC-721, ERC-1155 - token standards approved by Ethereum

Availability of Data and Materials

The data used in our research were obtained from reliable sources, and none of it was self-constructed. All data can be accessed through the references provided in our paper. This research utilized these sources to review financial scenarios involving quantifiable metrics and data.

Competing interests

The author declares no conflict of interest.

Acknowledgements

Acknowledgement to The International Journal of Blockchain Technologies and Applications for collaboration and consideration. Following acknowledgement to the Stanford Journal of Science, Technology and Society for collaboration and consideration.

References

[1] Decentralized Internet. *DigitalOcean Documentation*. [Online]. Available: https://docs.digitalocean.com/products/marketplace/catalog/decentralized-internet/
[2] (28 June 2021). First looks into Interplanetary File System. *Storage Gaga*. [Online]. Available: http://storagegaga.com/first-looks-into-interplanetary-file-system/. Accessed July 3 2022.
[3] Consistent Hashing. In this blog we will look at what is… | by Animesh Agarwal, *Medium*, 13 May 2020.
[4] Find sources: "Distributed hash table”. Wikipedia. [Online]. Available: https://en.wikipedia.org/wiki/Distributed_hash_table. Accessed 2 July 2022.
[5] Off-chain based data storage mechanism. | Download Scientific Diagram. ResearchGate. [Online]. Available: https://www.researchgate.net/figure/Off-chain-based-data-storage-

mechanism_fig4_339672569
[6] Decentralized Social Networking Protocol (DSNP). [Online]. Available: https://unfinished.com/wp-content/uploads/dsnp_whitepaper.pdf
[7] Blockstack Technical Whitepaper. *MIT PDOS*. (12 October 2017). [Online]. Available: https://pdos.csail.mit.edu/6.824/papers/blockstack-2017.pdf
[8] Storj Whitepaper V3. *Storj*. [Online]. Available: https://www.storj.io/whitepaper
[9] Rice, Damien, and Matt Galbraith. YouTube. [Online]. Available: https://www.sciencedirect.com/topics/computer-science/paillier-cryptosystem
[10] Helium Whitepaper. [Online]. Available: http://whitepaper.helium.com/
[11] W. John. "What is Zero-Knowledge Proof (ZKP)?" *E-Crypto News*.
[12] The Internet Computer for Geeks. *Internet Computer*. (19 April 2022). [Online]. Available: https://internetcomputer.org/whitepaper.pdf. Accessed 9 April 2023.
[13] M. Joel. "Stop Burning Tokens – Buyback and Make Instead — Placeholder." *Placeholder VC*, 17 September 2020.
[14] Whitepaper - Resources. Cosmos Network. [Online]. Available: https://v1.cosmos.network/resources/whitepaper