Proof of Abstraction: The Consensus Mechanism Driving Adoption, Powered by XION

Burnt Research

Draft-Release: December 3, 2024

Abstract

We introduce Proof of Abstraction, a novel consensus mechanism powered by the XION token to enable increased security through abstraction. Proof of Abstraction is developed to address the tradeoff between security and accessibility inherent in traditional Proof of Stake implementations. Anchored in XION's User-Security Symbiosis Rubric, it shifts the emphasis from purely wealth-based influence to user-experience as a primary vector for network security and value distribution. Proof of Abstraction incentivizes network growth by aligning participant rewards with the network's primary goal – lowering user-complexity barriers and enabling broader accessibility. XION's Generalized Abstraction is purpose built to provide builders the tools to abstract away complexities, and through Proof of Abstraction, aligns network incentives to increase chain security. As abstraction drives adoption, the XION token usage increases, subsequently increasing network security, incentivizing increased abstraction, and further driving adoption. We outline the conceptual foundation of Proof of Abstraction, demonstrating how the XION token underpins the system to enhance network security and, more importantly, to facilitate widespread adoption. We further extend this to connected ecosystems, effectively positioning the XION token as a universal conduit for industry adoption.

1 Introduction

Proof-of-Stake consensus mechanisms have revolutionized secure, scalable decentralized computing through the introduction of cryptoeconomic security. However, the tension between security requirements and user accessibility continues to present a critical challenge for their broader adoption. Proof of Stake networks have historically struggled to properly align network incentives between the network's ultimate goal and the action that drives the highest rewards. This lends itself to concentrating governance power in the hands of a few token-rich entities, ultimately undermining network security and decentralization.

Additionally, Proof of Stake mechanisms rely on native tokens, integral components of decentralized computing architectures, serving as the foundation for incentive structures and security mechanisms. While native tokens have been instrumental in securing these systems against various attack vectors, they have simultaneously hindered widespread adoption. The inherent complexities associated with these tokens have introduced significant friction points in the user experience. These technical barriers have proven to be a substantial impediment to the mainstream adoption of Web3 applications, effectively limiting their reach beyond the technically adept early adopters.

This paper examines the novel dynamics of Proof of Abstraction, uniquely enabled by XION's infrastructure innovations, and powered by the XION token. It explores its origins and necessity in an industry that has historically struggled with adoption. Proof-of-Abstraction aligns network participant incentives,

while XION's protocol-level abstractions enable the XION token to strengthen the economic security of the network without hindering end-user experience. By rewarding contributions that directly support ecosystem growth, Proof of Abstraction ensures that its security model serves a higher purpose: building a scalable and accessible network that thrives through adoption rather than accumulation.

The remainder of the paper is structured as follows: Section 2 provides background on the fundamentals of Proof of Stake systems and their unintended alignment and user-experience issues; Section 3 presents the User-Security Symbiosis Rubric as a solution for aligning security with user accessibility; Section 4 introduces Proof of Abstraction and the XION token's crucial role in enabling its novel mechanism; Section 5 positions the XION token as a universal conduit for industry adoption; and Section 6 concludes.

2 Background

While Proof of Stake has improved upon the energy efficiency and scalability limitations of Proof of Work, it still faces key challenges. The background section elucidates the foundational concepts that gave rise to Proof of Abstraction, establishing the critical need for a mechanism that aligns network security with broader adoption by incentivizing user and developer behaviors that add value to the network's security, scalability, and decentralization. By exploring the limitations of current models, we set the stage to introduce the novel experience-driven security framework and position Proof of Abstraction as the solution to addressing pervasive adoption issues in Web3.

2.1 The Decentralization Triangle

Developed in response to Bitcoin, the decentralization triangle (Figure 1) details the trade-offs between scalability, security, and decentralization — foundational challenges blockchain networks must balance to function effectively in a trustless environment. The PoW consensus mechanism,

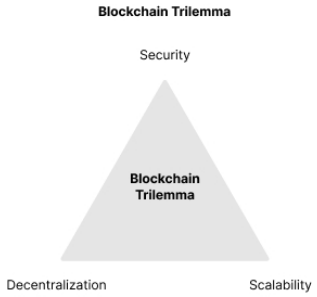

Figure 1: The Decentralization Triangle

while effective in addressing the Byzantine Generals Problem, often compromises one of these elements to achieve the others. For example, prioritizing security and decentralization but lacking scalability due to the high computational costs required to validate transactions and low throughput.

Security in the triangle refers to the protocol's ability to defend against attacks and breaches while ensuring the integrity of the transactions on its ledger. Strong security is achieved by implementing a resilient consensus mechanism that deters the chain against attacks. For instance, PoW networks like Bitcoin rely on high computational power to make it prohibitively costly for any single entity to alter the blockchain. A secure network ensures immutability and trustworthiness, making it a cornerstone of blockchain adoption. However, the decentralization triangle implies that focusing on security often necessitates slower transaction times and higher fees to prevent overload, limiting scalability.

Scalability in the triangle is the network's capacity to handle a high volume of transactions efficiently. In blockchains, achieving scalability without compromising security or decentralization has remained a challenge. PoW networks, for example, are inherently limited in transaction throughput due to their reliance on computational power and block interval limits. Layer 2 solutions, sidechains, and alternative consensus mechanisms, like Proof of Stake, are often built on top of networks to scale

them up. While these solutions can address immediate throughput challenges, they may shift network dynamics toward centralization. For instance, Layer 2 providers, sidechain operators, and Proof of Stake validators are often limited in number, concentrating decision-making power among a select few.

The Web3 industry is built on the promise of decentralization — the principle that no single entity or group should control a network, allowing it to remain inclusive to all. In a decentralized blockchain, multiple nodes independently validate transactions, ensuring trust and transparency without a central authority. Decentralization is also essential for resilience, as a distributed network can withstand attacks more effectively and operate in a trustless environment. But maintaining high levels of decentralization can hinder scalability, as each node must process and agree on every transaction. This makes it difficult for networks to scale efficiently.

2.2 Proof of Stake Fundamentals

Introduced in 2012, Proof of Stake aligns validators' economic interests with network stability through a stake-based approach, making attacks prohibitively expensive. Key components of Proof of Stake networks include validators, staking mechanisms, consensus protocols, and slashing penalties for rule violations. Validators propose and validate blocks, while token holders participate in consensus by locking tokens as collateral. Economic incentives, such as rewards and penalties, align participant behavior with network goals, and governance mechanisms enable protocol upgrades. Utility tokens are central to Proof of Stake networks, facilitating staking, validation, governance, fee payment, and economic alignment among participants. By integrating these elements, Proof of Stake networks attempt to create sustainable, scalable foundations for app builders and long-term growth.

2.2.1 Fees

Transaction fees serve a dual purpose in Proof of Stake networks: they compensate validators for the computational resources expended in processing transactions and incentivize validators to prioritize certain transactions over others. To quantify the computational cost associated with a transaction, the concept of "gas" was introduced. The payment of fees to cover gas costs is a fundamental feature of Proof of Stake utility tokens. The precise calculation of gas costs may vary across networks, but most implementations include two components: 1. A "base fee" to cover the basic computational expenditure, and 2. A "priority fee" that functions as an incentive for validators to include the transaction. In the Ethereum network, for example, the total fee is calculated using the following equation:

$TotalFee$ = Units of gas used $\times$ (Base fee + Priority fee)

The units of gas used are determined by the computational complexity of the transaction, while the base fee is dynamically adjusted based on network conditions, such as recent block congestion. The priority fee is set at the discretion of the user. Although a transaction without a priority fee is technically valid, it may not be promptly included in a block, as validators have little incentive to prioritize it. Gas costs are denominated in the native token of the Proof of Stake network. Consequently, both the base fee and priority fee are priced relative to the value of a single unit of gas in terms of the network's native token.

2.2.2 Staking and Validating

In Proof of Stake systems, validator selection is typically proportional to the amount of tokens staked. Participants must lock a minimum quantity of tokens to qualify as validators, a mechanism that serves to align economic incentives within the network and provide a form of economic security against malicious behavior. The probability of a validator being chosen to propose a block often correlates with their stake size, creating a system where larger stakeholders have a higher likelihood of block production and subsequent rewards. This approach ensures that those with the most to lose

from network failure are also those most likely to be responsible for its maintenance. The general formula for the probability of a given staker being selected is as follows.

$$P(Selection) = \frac{StakeAmount}{TotalAmountStaked}$$

Modern Proof of Stake systems often use a multi-round voting process for consensus. A validator is chosen to propose a block, which is then voted on by others. Validators prevote for valid proposals or abstain (NIL). If a block receives over two-thirds of prevotes, it is precommitted; otherwise, NIL is precommitted or the process continues.

Validators earn rewards through inflation (new token issuance) and transaction fees but risk slashing if they violate network rules. This penalty ensures validators act in the network's best interest, maintaining security and integrity.

2.2.3 Governance

Governance in Proof of Stake blockchains drives network evolution, using native tokens for decentralized voting on proposals like upgrades, parameter changes, and fund allocation. Validators and, in some networks, delegators vote proportionally to their staked tokens, with proposals passing upon meeting quorum and approval thresholds. This model aligns stakeholder interests with the network's future.

2.2.4 Token Dynamics (Minting)

Minting dynamics govern how new tokens are issued and their impact on the network's inflation rate. Validators earn rewards through transaction fees and block subsidies, which consist of newly minted tokens.

2.3 Proof of Stake Issues

In Proof of Stake, a validator's influence is directly tied to the amount of cryptocurrency they stake. The more assets staked, the greater the validator's power over block proposals, validation, and network decisions. Validators are incentivized to act honestly, as dishonesty results in penalties and loss of staked assets. However, this structure favors wealthier participants who can stake more, earn greater rewards, and further consolidate their control over the network. Over time, this creates economic centralization, undermining blockchain's decentralization goals.

This concentration of power discourages smaller stakers and new participants, limiting diverse participation and decentralization at scale. Additionally, the proliferation of Proof of Stake chains has amplified these issues. While new chains promise unique features, they often prioritize rewards for large holders rather than contributors who drive adoption. This dynamic perpetuates barriers to user adoption and hinders the industry's ability to build engaged user bases. Below are additional examples of these challenges.

2.3.1 Token Procurement

The acquisition of native tokens in Proof of Stake networks imposes a high technical threshold before users can interact with Web3 applications. This process typically requires engagement with centralized or decentralized exchanges, where users must first establish accounts—often involving stringent know-your-customer (KYC) procedures that can delay activity for several days. If the desired native token is not directly available on an exchange with fiat on-ramp capabilities, users must acquire an intermediary token like USDT, introducing additional complexities such as understanding trading pairs and navigating decentralized exchanges (DEXs). This necessitates familiarity with various blockchain networks and exchange interfaces, which can be daunting for newcomers.

2.3.2 Storage and Wallets

Following token acquisition, users face the challenge of selecting and setting up an appropriate wallet for secure storage and network interaction. The multitude of wallet options—varying in security features, user interfaces, and blockchain compatibility—makes

the selection process complex and overwhelming. Users must ensure that the chosen wallet not only supports the desired network but also provides robust security measures. The setup involves managing private keys and seed phrases, concepts that are often unfamiliar and intimidating to first-time users. Mismanagement of these cryptographic credentials can lead to irreversible loss of funds, presenting a significant risk.

2.3.3 Gas Fees

Gas fees introduce another layer of complexity for users interacting with Proof of Stake networks. Users must grasp the concept of gas as a unit of computational work necessary for transaction processing, which is often an unfamiliar abstraction. Managing gas fees requires understanding dynamic pricing mechanisms influenced by network congestion and computational demand. Incorrect fee settings can result in failed transactions or prolonged confirmation times, leading to wasted resources and user frustration. Although wallets may offer gas fee estimates, rapid fluctuations necessitate constant monitoring and adjustments, adding to the cognitive burden on users.

Furthermore, variations in gas fee structures and denominations across different networks complicate cross-chain interactions. Users must familiarize themselves with each network's specific fee models, which can be confusing and error-prone. The volatility and unpredictability of gas fees hinder the user experience, especially for those accustomed to the seamless interfaces of Web2 applications. These complexities not only deter end-users but also limit the market potential for developers, as they restrict the user base to individuals familiar with blockchain intricacies.

Collectively, the challenges associated with gas fees contribute to a user experience that is less accessible and more cumbersome than centralized alternatives, impeding broader adoption of Proof of Stake networks and decentralized applications (Figure 2).

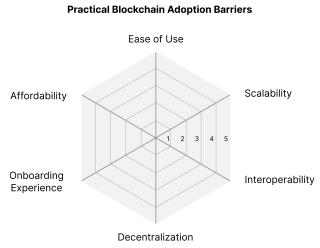

Figure 2: Barriers to Widespread Adoption

2.4 Web3 Fragmentation Problems

Beyond user adoption challenges, fragmentation stands as one of the most significant issues within the current Web3 ecosystem. To make Web3 appealing to the mass market and unlock new market opportunities, it is imperative to render these segregated chain environments composable with one another while abstracting away the complexities associated with their utilization.

However, the challenges associated with utilizing native tokens are amplified in a multi-chain environment. Users who wish to interact across multiple chains must contend with procuring and managing multiple native tokens, as each network requires its own token for transaction fees and interactions. This necessitates that users acquire the tokens of every network they intend to use and comprehend the intricacies of paying gas fees on each network, with each having distinct rules and pricing mechanisms.

3 The User-Security Symbiosis Rubric

New challenges have emerged as Proof of Stake networks have evolved. Namely, maintaining an optimal balance among decentralization, security, and scalability becomes increasingly difficult as governance power becomes more concentrated among those who stake the most tokens. While Proof of Stake has managed to address some scalability concerns, it has also introduced unintended consequences

to decentralization, and as a knock-on effect, to security. In addition, the existence of a native token for each network has introduced unintended user experience hurdles that have further exacerbated adoption challenges.

The User-Security Symbiosis Rubric (USSR) aims to realign incentives to promote network behaviors that drive adoption, and subsequently network security.

3.1 Incentive Compatibility

Incentive Compatibility is a state in economics where the participants are motivated to act in accordance with the outcome they desire. Within a larger system like a blockchain network, an incentive-compatible consensus mechanism would be one where every participant's optimal choice aligns with the desired outcome of the entire system. This ensures that working to receive their incentives leads to the intended result for the system as a whole.

In the current Proof of Stake model, network participants are more incentivized to lock up their tokens than they are to contribute to the network's growth. To address the shortcomings of Proof of Stake, the incentive system of a blockchain network should therefore reward the overarching goal of each system — maintaining a balance between decentralization, security, and scalability to accommodate more users and increased activity. With onboarding users as the driving force behind creating secure, decentralized, and scalable systems, it is this process that should be incentivized to maintain the long-term viability of a blockchain. Embedding the pursuit of new users within the blockchain's incentive model achieves numerous outcomes that will have far-reaching implications for the future of the industry;

1. As a chain's user base expands, network participants are incentivized to strategize and change tactics to continue onboarding more users. This means participants are incentivized to address user experience pitfalls within the network instead of holding and staking large amounts of tokens. As the user base increases, participants who are responsible for driving this growth receive a portion of rewards based on their efforts to enhance user experience through abstraction (e.g., improving network accessibility and simplifying onboarding processes). This incentivizes individuals to optimize both their approach and the platform's usability, rather than just increasing their stake.

2. Incentivizing participants who actively strategize and revisit their approach to getting rewarded to address the chain's user experience make way for innovation within the broader industry. The blockchain network can incentivize active strategy shifts through performance-based rewards that focus not just on token staking, but on how well participants innovate in response to the users' evolving needs.

3. Voting power is distributed to those who add the most value to the network, ensuring that participants who add the most value — not just those who hold the most tokens — have more influence over decisions. This encourages a more decentralized and fair governance model that prioritizes the network's growth, security, and user experience over token hoarding.

With this in mind, we propose the User-Security Symbiosis Rubric (USSR) based on addressing the blockchain trilemma using incentive compatibility.

3.2 Network Participant Alignment Framework

The User-Security Symbiosis Rubric addresses the shortcomings of Proof of Stake systems while tackling the pressing issue of user adoption that existing networks haven't addressed. The User-Security Symbiosis Rubric establishes a reciprocal relationship between user engagement and network security. As Proof of Stake networks continue to evolve, they often face challenges related to centralization and barriers to participation, which can deter new users from joining and actively contributing to the ecosystem. This framework recognizes that for Proof of Stake

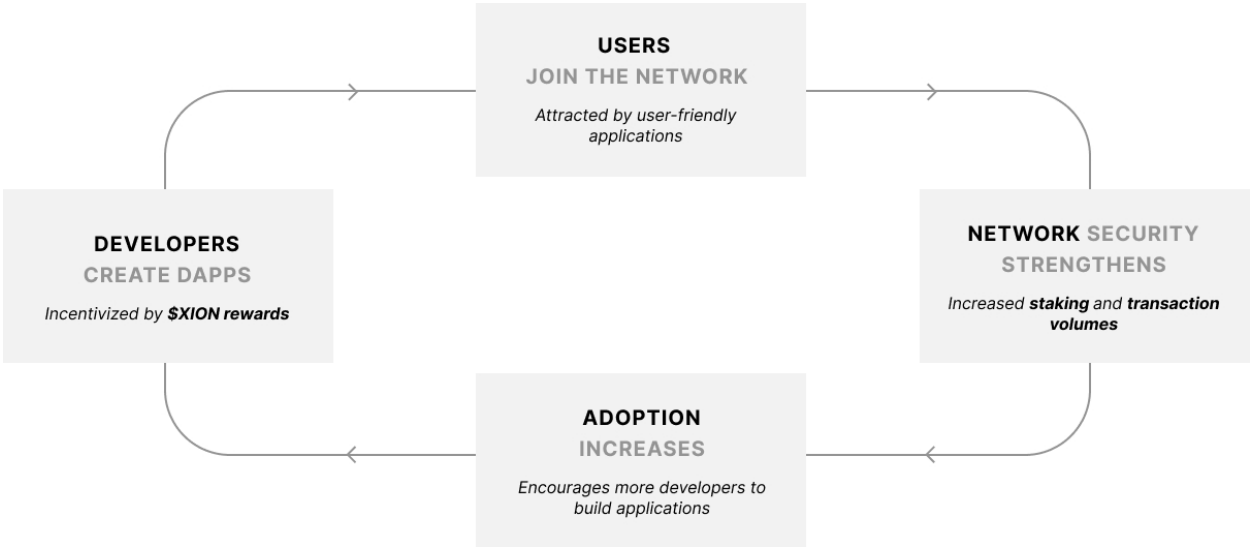

Figure 3: User-Security Symbiosis Rubric

to thrive, it must not only incentivize validators to maintain network integrity but also empower users by aligning their interests with the overall security and functionality of the blockchain.

1. Abstraction → Enhanced user experience, lowering barriers to entry and making the platform accessible to a broader audience.
2. Better Experience → Improved user retention and satisfaction, encouraging more users to engage and participate.
3. More Users → Increased active participation reinforces network security and strengthens decentralization.
4. More Value → Elevated network security attracts further development of high-quality applications through increased incentives.
5. More Abstraction → Developers are incentivized to innovate, further improving the user experience and beginning the cycle anew.

At its core, the User-Security Symbiosis Rubric advocates for an approach where user activity is intricately tied to overall network security. Through increased user activity, the demand for the XION token utility token increases, further securing the network.

At scale, the User-Security Symbiosis Rubric also has the potential to address key adoption hurdles in the industry. It pushes developers to take the lead in creating seamless, interoperable applications that abstract away user complexities. With incentives directly tied to the activity that they drive to the network, developers are compelled to ensure that their applications attract and retain a high level of user activity. As the network grows, new equilibrium points will emerge as developers are incentivized to meet user needs at all times, creating a "survival of the most secure and user-friendly" dynamic.

Literature exploring the rise of the internet has highlighted the importance of network effects in enabling a technology to reach a critical mass which propels it into mainstream usage. Proof of Abstraction is the implementation of the User-Security Symbiosis Rubric, designed to maximize the number

of potential interactions between Web3 entities and also minimize the friction associated with these interactions. Such a design is favorable to accessing network effects and reaching the critical mass needed to bring Web3 technology to a mainstream audience by solving its key challenges.

4 Proof of Abstraction, Powered by XION

Proof of Abstraction is a novel consensus mechanism powered by the XION token to enable increased security through abstraction. It is developed to address the tradeoff between security and accessibility inherent in traditional Proof of Stake implementations. It does this by aligning a new incentive mechanism with core protocol-level abstraction infrastructure, through the XION token. In the sections below, we explore both: 1) the incentive alignment mechanism and 2) the protocol-level abstractions driving adoption.

4.1 Incentive Alignment

Proof of Abstraction incentivizes developers to create applications and features that simplify blockchain interactions, thereby expanding adoption, driving demand for the XION utility token, enhancing network security, and initiating a self-reinforcing growth cycle. Network participants who achieve key outcomes are rewarded with XION governance tokens commensurate with their success, providing them with influence proportional to their contributions. This mechanism creates a more user-driven ecosystem, wherein abstraction attracts new users, increased user adoption elevates demand for the XION token, and heightened demand further strengthens network security. The XION token thus aligns participants across multiple facets as detailed below: staking, governance, minting, and fees.

4.1.1 XION Staking & Network Security

The security of the blockchain is underpinned by the total economic value of all staked XION tokens. The network relies on validators to maintain its integrity, with the XION token serving as the foundation for its economic security. Through Proof of Abstraction, increased network activity is propelled by heightened levels of abstraction, which ultimately increases network security.

One of the principal drawbacks of traditional Proof-of-Stake networks is the overincentivization of staking at the expense of active network participation. Proof of Abstraction mitigates this issue by aligning participant rewards with the network's primary objective—reducing user-complexity barriers and promoting broader accessibility. A portion of the network's token emissions is allocated to participants who most effectively drive user adoption. This creates new dynamics whereby stakers are incentivized to also be active participants in the network in order to maximize rewards. The reallocation is a progressive process, initially occurring off-chain and gradually being integrated directly into the protocol and on-chain governance.

4.1.2 XION Governance

The XION token holders actively participate in network governance by submitting and voting on proposals, thereby aligning individual interests with the overarching objectives of the network. However, governance decisions often become concentrated among participants who have accumulated the most tokens, regardless of their actual contributions to the network's goals.

Proof of Abstraction addresses this issue by incentivizing participants who actively advance the network's primary objectives, thereby enhancing their decision-making power. This creates a positive feedback loop that reinforces valuable contributions and improves overall network governance. It aligns developers with end-user needs, distributing the XION tokens (and therefore power) based on active contributions rather than purely token holdings. As new users join, network security improves through the XION token emissions that reward developers who build abstracted applications driving high user

Comparison Chart of Blockchain Generations: From PoW to PoA

	Proof of Work	Proof of Stake	Proof of Abstraction
Energy Efficiency	Low	Medium	**High**
Scalability	Low	High	**High**
User Incentives	None	Moderate	**Strong**
Security	High	Medium	**High**

Figure 4: Proof of Abstraction v. Predecessors

activity, and supporting long-term viability.

$$T_{Abstraction} = T_{minted}(IR \times A)$$

In the above equation, $T_{Abstraction}$ is the total amount of tokens allocated to incentivizing abstracted app development, IR is the inflation rate, A is the percentage of the emission which will be allocated to the Proof of Abstraction mechanism, and T_{minted} is the tokens minted. This mechanism embeds an incentive structure in the XION token which spurs the development and advancement of apps that provide utility and a seamless user experience to the broader mainstream market.

4.1.3 XION Minting Dynamics

The minting dynamics of a native token are integral to the functioning and long-term viability of the network. It is paramount that the minting of a token is designed to facilitate its intended usage while also providing stability in the network. A token with excessive inflation will incentivize active usage but will eradicate holder wealth, disincentivizing long-term storage and price stability. A deflationary or disinflationary token will incentivize long-term storage but will typically deter users from actively utilizing the token, a dynamic which is unfavorable for Web3 network tokens. The XION minting dynamics were designed from a first-principles approach to facilitate active usage within Web3 applications while also developing a sufficient holder base which would help bring price stability and long-term user growth to the protocol. XION deviates from typical minting dynamics in two major ways;

1. Accumulated fees are used to offset inflation when possible
2. Token inflation is calculated against staked tokens only

The XION token minting is operated via the minting module. The module functions via parameters which maintain a predetermined ratio of staked versus liquid tokens within the ecosystem. There are three parameters: the upper bound for inflation, the lower bound for inflation, and the target staking ratio. The target staking ratio will be determined via developer proposals and the parameters are also subject to change via approved proposals. The parameters are in place to ensure a balance is maintained between the number of staked tokens and the liquid tokens in the marketplace. Changes in the inflation rate will be moderated by the following equations.

4.1.4 Token Inflation Applied to Staked Tokens

The predominant model for inflation among Proof of Stake tokens is to apply inflation to the total supply

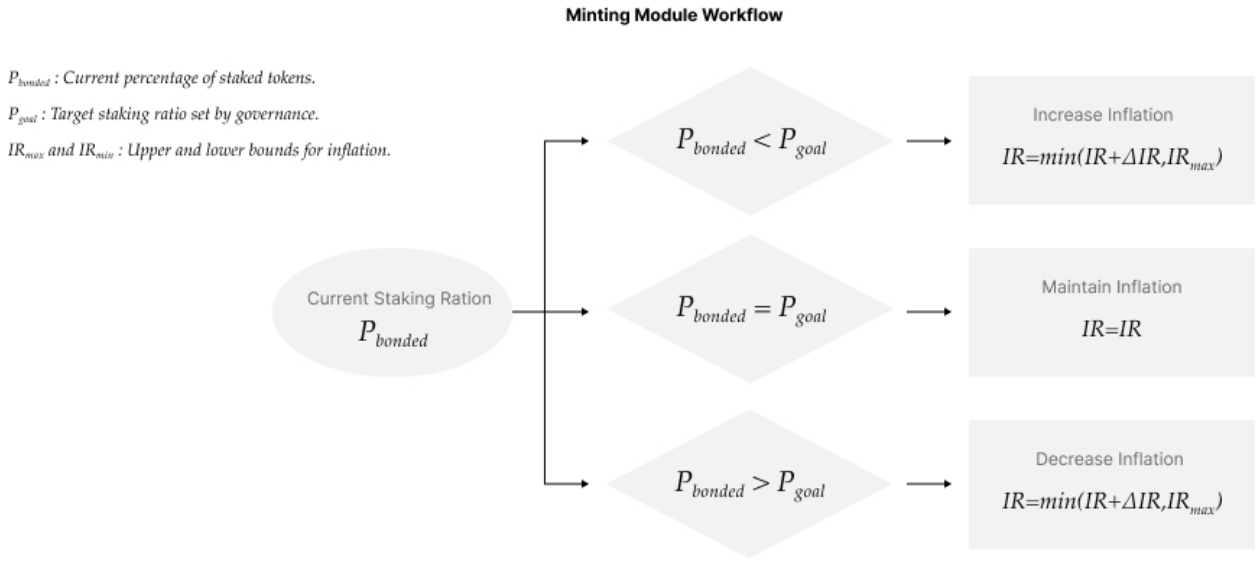

Figure 5: Minting Module

of tokens. This creates a disparity between the inflation rate in regards to the total supply of tokens and the annual percentage yield which validators earn on their staked tokens. XION implements a model whereby the inflation is calculated solely on staked tokens, aligning the overall inflation rate with the annual percentage yield of staked tokens and also benefiting the XION token holders by reducing the amounts of new XION tokens issued. The relation is expressed in the following equation.

$$T_{minted} = IR \times T_{bonded}$$

In the above equation, T_{bonded} is the total XION tokens bonded. This reduces the overall inflationary impact and stakers will observe that their APY is equal to the inflation rate. This creates an environment to attract long-term network participants, as opposed to validators which will switch their resources based on which Proof of Stake network is offering the highest APY.

4.1.5 XION Fees

As the native token of the Layer 1 blockchain, the XION token is utilized for paying network transaction fees. This intrinsic utility ensures that all operations, including transactions and smart contract executions, are facilitated using the XION token, thereby reinforcing its fundamental role within the network's economic framework. It is important to note that through Proof of Abstraction, the XION token is abstracted away from the end-user's perspective – it maintains its inherent security attributes without introducing complexity or hindrance to the end-user. The exact dynamics are detailed in Section 4.2.1 below.

4.2 Protocol Level Abstractions Driving Adoption

Proof of Abstraction is made possible through XION's key infrastructure innovations, namely its protocol-level abstractions. By reducing the friction

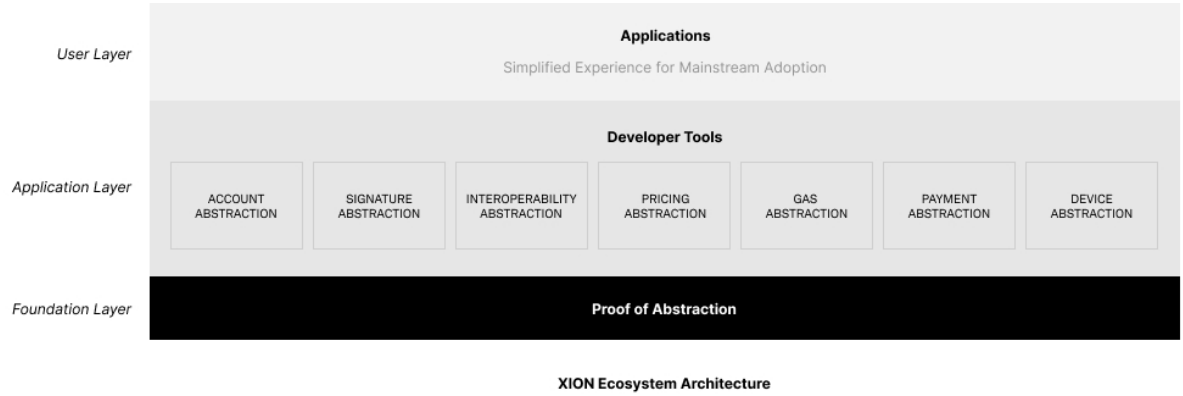

Figure 6: XION Ecosystem Architecture

commonly associated with Web3 interactions, this infrastructure enables seamless user onboarding while preserving the high standards of decentralization and security required for sustainable scalability. This creates a positive feedback loop: abstractions lead to more users, which increases network security, attracts more developers, drives increased development and abstraction, driving further adoption and security.

This model, combining the right incentive mechanism with powerful infrastructure (Figure 6), ensures that the network's growth is directly linked to enhanced security and usability without compromise. This positions the chain to be extremely scalable, secure, and user-centric. Below, we cover 1) XION's innovative Account Architecture, and 2) XION's fee abstraction.

4.2.1 Account Architecture

In keeping with Proof of Abstraction's end goal to onboard users at scale, XION has built robust protocol-level chain abstraction functionalities to empower developers with the tools they need for their applications to align with the needs of users and achieve long-term viability. Its account architecture is made up of three key pieces: 1) Meta Accounts, 2) Sessions Keys, 3) an Authorization Framework.

4.2.2 Meta Accounts

Meta Accounts are central to XION's account architecture, implementing protocol-level account abstraction to improve user experience, security, and programmability. They are designed to facilitate seamless usage of applications, with the XION token and other typical Web3 complexities abstracted away. They are a key tenant of the Proof of Abstraction flywheel, facilitating many of the advanced abstractions necessary to onboard users. Meta Accounts facilitate secure interactions with applications through the novel use of Sessions Keys paired with an Authorization Framework (Figure 7).

4.2.3 Session Keys

Session Keys are temporary, limited-privilege cryptographic keys that enhance security and user experience. These keys allow users to interact with Web3 apps securely without exposing their primary Meta Account assets. Their ephemeral, limited nature reduces the risks of private key compromise, as unauthorized access is constrained by session-specific permissions. Session Keys can perform specific functions within Meta Accounts and use the XION token or cross-chain native tokens, with fee abstraction adding security and ease.

For users, Session Keys streamline interactions

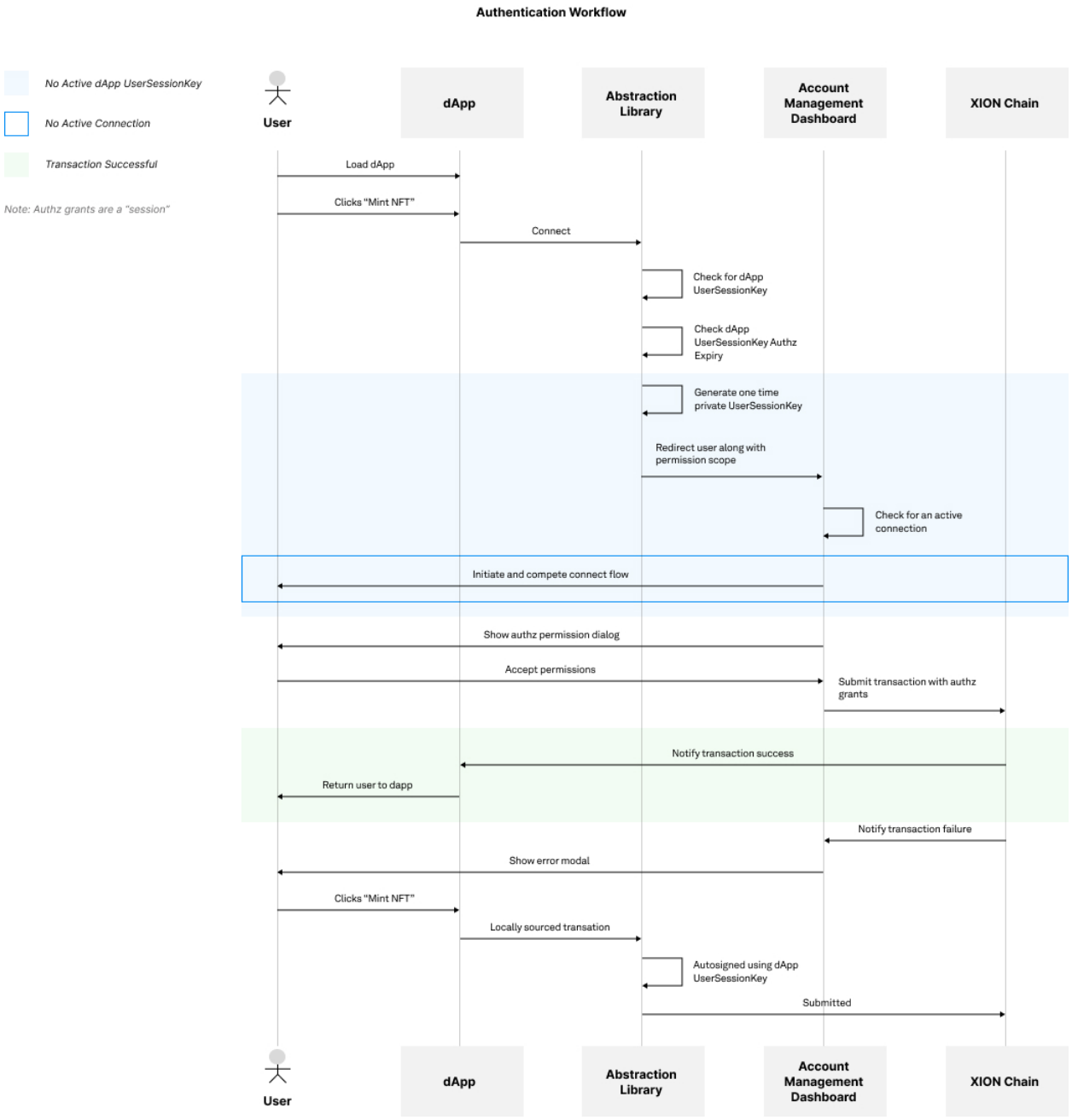

Figure 7: Authorization Framework

by eliminating the need for external wallet plugins and repetitive authentication. Transactions can be executed with a single action, and session bundling allows multiple transactions to occur without individual authentication. This simplifies the experience and aligns blockchain interactions with Web2 standards, improving onboarding and usability for new users. These interactions between Session Keys and Meta Accounts are facilitated by an advanced Authorization Framework.

4.2.4 Authorization Framework

XION manages Session Key permissions within Meta Accounts through an Authorization Framework. When a Session Key is generated, it requests specific permissions from the user's Meta Account, detailing its intended operations. Users can easily review, adjust, and revoke permissions at any time, ensuring granular control over what actions apps can perform. This approach minimizes security risks by adhering to the principle of least privilege and highlighting unusual permission requests.

The framework balances security and user experience by consolidating permission management within Meta Accounts, avoiding repetitive authentication while maintaining control. This design ensures that XION facilitates secure, seamless interactions, driving both application development and network security.

The module provides interfaces and messages to grant permissions for one account to act on behalf of another. A "grant" authorizes the grantee to execute specific messages (Msg) on behalf of the granter. The "authorization" itself is an interface that defines the rules and validation logic for executing these grants. Authorizations are highly flexible, enabling custom permissions for any Msg service method, even those outside the module where the Msg method originates.

Meta Accounts, Session Keys, and the Authorization Framework form a robust account architecture that enables the Proof of Abstraction growth flywheel by addressing the inherent challenges of traditional

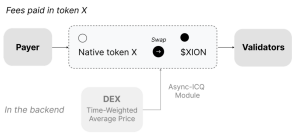

Figure 8: XION Token Fee Abstraction

interactions. Building upon this foundation, the next section explores how XION leverages its advanced account architecture to implement fee abstraction, a critical feature that eliminates one of the most significant barriers to user adoption in Web3 yet enables the XION token to accrue network security.

4.3 XION Fee Abstraction

One of the persistent challenges in blockchain technology is the complexity associated with transaction fees, commonly known as "gas fees." These fees can pose a significant barrier to entry for new users, requiring them to acquire and manage native tokens solely for the purpose of paying transaction costs. Leveraging the advanced account architecture outlined in the previous sections, XION utilizes a fee abstraction mechanism that eliminates the need for users to hold or interact directly with the XION token when conducting transactions. This approach simplifies the user experience, enhances accessibility, and addresses key issues related to user adoption in the Web3 ecosystem while preserving the economic security of the network.

4.3.1 Delegated Fee Payments

XION's fee abstraction mechanism is intrinsically integrated into its account architecture, specifically through Meta Accounts and the Authorization framework. Delegated Fee Payments allow app developers to delegate the responsibility of transaction fee payment to themselves through a Treasury Contract. This delegation is then integrated directly into the Authorization Framework and Session Keys within Meta Accounts, whereby developers have granular cover over Session Key transaction fees. The app developer can then submit transactions and

pay the associated fees using the XION tokens they hold, abstracting the fee payment process from the user's perspective.

The predominant model for fee payment within Proof of Stake and other decentralized networks is to place the onus for payment on the end user, giving rise to a myriad of complexities and friction points associated with native token procurement, calculating the appropriate amount of fees, and paying the fees in a secure manner. The XION token provides an alternative model whereby developers can choose to pay the token fees on behalf of their users. Through an allowance module, developers have broad control over how they can pay for user fees. On the user end, this allows for a seamless user experience where they can execute Web3 transactions while fees are paid on the backend. On the developer end, the control over the degree of which they want to cover fees allows them to protect against attacks such as entities wishing to drain their funds.

XION development libraries provide additional control, allowing developers to create custom transactions around authorization executions. For example, developers can pre-code transactions to gift tokens once a Meta Account generates a Session Key. They can also reference third-party chains or applications and control fee coverage based on external activity thresholds.

Developers who effectively use Delegated Fee Payments and other functionalities, like pre-coding transactions, to build abstracted apps that drive user adoption will be rewarded through the Proof of Abstraction incentive mechanism. By leveraging XION's abstraction features, developers can attract more users, competing for rewards by building applications that provide the best user experience.

4.3.2 Token-Agnostic Fees

Token-Agnostic Fees enable users to pay transaction fees without holding the native XION token. Through built-in exchange mechanisms and fee conversion modules at the protocol level, the network accepts alternative tokens and internally converts them to the XION token for fee settlement. This allows users to transact using tokens they already possess, such as stablecoins or other widely held cryptocurrencies, without the need to acquire the XION token specifically for fee payment.

While the token-agnostic fee mechanism adheres more closely to the standard model of fee payment within Proof of Stake networks, it differs in the respect that it allows users to utilize any Web3 token for fee payment. Users can seamlessly carry out transactions and pay the appropriate fees without ever procuring the XION token, an important implementation of abstraction. It also allows for users to denominate their account in USD by making USDC or another USD-pegged stablecoin the predominant fee-paying token in their account, further smoothening the user experience and making the protocol more attractive to new users. Such a denomination would allow for a user experience which would be much more familiar to Web2 users who are familiar with carrying out online activities that are priced in a major fiat currency.

By combining Delegated Fee Payments and Token-Agnostic Fees, XION effectively decouples the act of transacting from the necessity of managing native tokens for fee payment. This design streamlines the user experience, reduces barriers to entry, and retains the economic security benefits inherent in a Proof of Stake system by ensuring that validators are compensated in the XION token.

4.3.3 Solving Native Token Hurdles

The fee abstraction mechanism solves the issue of acquiring the XION token for transaction fees, removing the complexity of token procurement and management. This lowers the entry barrier for new users who may be unfamiliar with cryptocurrency exchanges or token processes.

Users can transact in familiar currencies, like stablecoins, without needing to understand gas fees

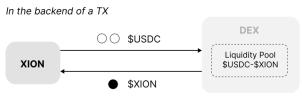

Figure 9: Token Agnostic Fees

or native token dynamics. This simplification aligns blockchain transactions with the seamless experiences expected from traditional financial systems, enhancing accessibility and supporting mainstream adoption.

By enabling users to transact with existing tokens or leverage fee delegation from apps, XION streamlines blockchain interactions, making them more user-friendly. This frictionless experience is key to promoting mainstream adoption, while XION's Proof of Abstraction rewards the development of such experiences, incentivizing the decentralized web.

5 The XION Token: A Universal Conduit For Industry Adoption

By combining advanced protocol-level abstractions with cross-ecosystem connectivity, Proof of Abstraction can be extended to all interconnected networks—effectively positioning the XION token as a universal conduit for industry adoption. Building upon its sophisticated account architecture and fee abstraction mechanisms, XION's cross-ecosystem abstraction addresses fragmentation within the Web3 landscape by enabling users to interact with various blockchain networks using a single Meta Account, without the necessity of managing multiple native tokens. This capability also empowers application developers on XION to build composable applications capable of leveraging functionalities across different networks.

This mechanism establishes ownership of SCAs on connected chains through cryptographic proofs and secure interchain communication protocols like the Inter-Blockchain Communication (IBC) protocol. When a user initiates a transaction for an external blockchain, the Meta Account packages the details and authorizations into a meta-transaction, which is relayed via IBC to the target chain, where the corresponding SCA executes it.

The XION token is central to this process, serving as the settlement medium between networks and as a critical component facilitating secure cross-chain composability. Fee abstraction can happen in multiple ways, without the end user needing to hold the XION token nor the destination chain token - a completely cross chain abstracted experience, increasing the XION token demand and subsequently network security.

The programmability of Meta Accounts further opens up the scope of possibilities regarding the development of composable cross-chain applications which are free of the typical complexities of Web3 apps. This vastly expands the rate at which the Proof of Abstraction incentive mechanism can spur growth, effectively transforming the XION token into a universal conduit for industry-wide adoption.

6 Discussion & Conclusion

Proof of Abstraction addresses some of Web3's most pervasive issues surrounding widespread adoption and useability by reorienting blockchain security around user experience rather than economic stake. By decoupling technical complexity from user interaction, the mechanism creates a positive feedback loop: increased user accessibility drives network participation, which builds security by allocating XION tokens and governance power to those that contribute the most to this dynamic by reducing entry barriers. XION's implementation of this consensus mechanism ensures that as more users engage with applications built on it, the network's security, reliability, and fault tolerance scale, reinforcing trust and demand for these applications. This in turn creates a flywheel effect in driving demand for the

XION token as the network expands and more users onboard.

XION's User-Security Symbiosis Rubric aims to motivate developers to build the most accessible, secure, and engaging applications to consistently meet the demands of users. Their strategies are supported by the architecture of XION's Meta Accounts giving application builders the foundational tools with which they can build useful and usable applications across a wide range of use cases and verticals. XION's incentive model is further strengthened by its architecture as it empowers builders to constantly iterate on their applications and benefit directly from a chain that grows in demand.

This flywheel effect also applies to all other chains as XION's userbase grows. XION's Meta Accounts are highly interoperable, meaning increased demand on XION has a direct impact on demand for other chains within its extensive ecosystem. This makes Meta Accounts a conduit for Proof of Abstraction and the XION token across numerous ecosystems at scale. XION's fee abstraction mechanism also plays a crucial role in reducing friction for users by abstracting fees using the XION token emissions. This user experience not only increases user adoption but also incentivizes developers to build apps that prioritize intuitive engagement, further fueling the adoption flywheel. As XION shifts from a purely wealth-based consensus model to one that rewards contributions to increasing network activity, Proof of Abstraction will catalyze adoption of XION Web3 overall.

References

1. V. Buterin and Y. Weiss, "ERC-4337: Account Abstraction Using Alt Mempool [Draft]," Sept. 29, 2021. [Online]. Available: https://eips.ethereum.org/EIPS/eip-4337

2. N. Mudge, "EIP-2535: Diamonds, Multi-Facet Proxy," Ethereum Improvement Proposals, Ethereum Foundation. [Online]. Available: https://eips.ethereum.org/EIPS/eip2535

3. F. Giordano, et al., "EIP-1271: Standard Signature Validation Method for Contracts," Ethereum Improvement Proposals, Ethereum Foundation. [Online]. Available: https://eips.ethereum.org/EIPS/eip-1271

4. J. Zhang and M. Wu, "Cooperation Mechanism in Blockchain by Evolutionary Game Theory," Wiley Online Library, Nov. 8, 2021. [Online]. Available: https://onlinelibrary.wiley.com/doi/10.1155/2021/1258730

5. X. Li, Q. Liu, S. Wu, Z. Cao, and Q. Bai, "Game theory based compatible incentive mechanism design for non-cryptocurrency blockchain systems," Journal of Industrial Information Integration, Dec. 23, 2022. [Online]. Available: https://doi.org/10.1016/j.jii.2022.100426

6. P. Daian, S. Goldfeder, et al., "Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges," in 2020 IEEE Symposium on Security and Privacy (SP), 2020, pp. 914–931.

7. V. Buterin, "A next-generation smart contract and decentralized application platform," Whitepaper, 2014. [Online]. Available: https://ethereum.org/en/whitepaper/

8. D. Johnson, A. Menezes, and S. Vanstone, "The Elliptic Curve Digital Signature Algorithm (ECDSA)," IJIS 1,

36–63 (2001). [Online]. Available: https://doi.org/10.1007/s102070100002

9. I. Liusvaara and S. Josefsson, "RFC 8032 Edwards-Curve Digital Signature Algorithm (EdDSA)," Internet Engineering Task Force, Jan. 2017. [Online]. Available: https://rfceditor.org/rfc/rfc8032

10. S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," Bitcoin. [Online]. Available: https://bitcoin.org/bitcoin.pdf

11. A. Yakovenko, "Solana: A new architecture for a high-performance blockchain v0.8.13," Solana Foundation. [Online]. Available: https://solana.com/solanawhitepaper.pdf

12. Cosmos Network, "Authorization and Grant," Cosmos SDK Documentation. [Online]. Available: https://docs.cosmos.network/v0.46/modules/authz/01$_c$*oncepts.html*

13. A. Hamlin, "Secure Multiparty Computation," Comp 116, Tufts University. [Online]. Available: www.cs.tufts.edu/comp/116/archive/ahamlin.pdf

14. J. Kwon and E. Buchman, "A Network of Distributed Ledgers," Tendermint. [Online]. Available: https://v1.cosmos.network/resources/whitepaper

15. L. Lyu, "abstract-account," GitHub repository. [Online]. Available: https://github.com/larry0x/abstract-account

16. A. Raja and E. Saradar, "Asynchronous Interchain Query Module (Async-ICQ)," GitHub repository, Aug. 30, 2022. [Online]. Available: https://github.com/strangeloveventures/async-icq

17. J. Allaire and S. Neville, "Introducing USD Coin (USDC) a Fully Reserved Stablecoin," Circle Blog, Sept. 26, 2018. [Online]. Available: https://www.circle.com/blog/introducing-usd-coin

18. T. Yun, S. King, and J. Lee, "Cosmos/ibc ICS027: Interchain Accounts Specification," GitHub repository. [Online]. Available: https://github.com/cosmos/ibc/tree/main/spec/app/ics027-interchain-accounts

19. C. Goes, "The Interblockchain Communication Protocol: An Overview," Interchain GmbH. [Online]. Available: https://arxiv.org/pdf/2006.15918.pdf

20. Abacus Works, "Hyperlane v3 Docs," Abacus Works, 2023. [Online]. Available: https://docs.hyperlane.xyz/