Intuition: The Trust Protocol

A decentralized system for reputation, trust, and decision-making in P2P systems.

William Luedtke
Intuition

Thursday 4th July, 2024

Abstract

In our migration to increasingly objective trust systems, the Intuition protocol emerges as a response to a critical challenge: the continued reliance of decentralized systems on social consensus and trust in humans. By decoupling complex data from both minds and platforms and streamlining it into a semantic, transparent, open, and verifiable framework, Intuition helps remediate the issues presented by this trust paradox by empowering users to achieve asymptotically probabilistic levels of trust based on readily available, relevant, relative, trusted, and contextual information. The result is a paradigm shift in society's interaction layer, adding additional context to decision-making processes to foster more secure and reliable interactions, ultimately paving a path toward a more holistic programmatic trust stack.

1 Introduction

The evolving landscape of the decentralized web is rooted in a paradigm shift from subjective trust to objective, system-driven trust mechanisms. The advent of platforms such as Ethereum has solidified the concept of trustless computation, yet this is merely one layer of a multifaceted trust paradigm. Ethereum, analogous systems, and their constituent pieces predicate a significant amount of security on social consensus that, paradoxically, tethers trust to human reliability. As an example - for the everyday user, interacting with decentralized protocols and smart contracts involves placing trust in select groups of developers. Even extant Decentralized Autonomous Organizations (DAOs), while innovative, often fall short of their titular promise, being neither fully decentralized nor autonomous and remaining extremely susceptible to human error and manipulation.

Despite the assurances of code executing with atomic precision, there remains an absence of efficient mechanisms for ascertaining trust in the entities that constitute and operate within these frameworks. This lacuna has been exploited to orchestrate large-scale misappropriations of funds, undermining the usability and integrity of the decentralized web.

To address the absence of trust and verification methods within these frameworks, we propose Intuition - an additional layer of the decentralized web that seeks to operationalize trust through a crowdsourced, semantic, verifiable social and knowledge graph. The Intuition system aims to refine decision-making akin to enhancing intuitive judgment, fostering a more reliable interaction layer. By extracting relevant data from both people and platforms and restructuring it into a cohesive and transparent framework, Intuition aims to reinforce the web's robustness and trustworthiness, enabling users to better approximate probabilistic levels of trust based on verifiable user-centric data and analytics.

Crucially, Intuition acknowledges that the future of knowledge is not a single monolithic truth, but an intersubjective prism reflecting a spectrum of perspectives, validated against a communal, immutable ledger. While the Web2 paradigm of disparate, fragmented, unstructured, filtered, and unstandardized data makes the task of data reconciliation difficult, the Intuition protocol leverages novel Web3 primitives to encourage the participation, convergence, and consensus of system participants. This approach allows for the coexistence of diverse individual realities, each buttressed by the cryptographic integrity of shared data. Such a system is invaluable in the context of many emerging technologies such as artificial intelligence, where

Archived copy · cryp2nova.com

the efficacy of these systems is predicated on the depth, source, and verifiability of the underlying data. Intuition equips technologies such as AI with a dataset that is not only structured, open, and verifiable, but also enriched with the breadth of human experience and intuition, ensuring that decision-making processes are both informed and resistant to monopolistic control.

1.1 Rationale

The impetus for the Intuition system stems from a critical examination of the current state of digital trust. As we navigate through the digital age, the mechanisms that govern trust and reputation in online interactions have become increasingly pivotal. Traditional centralized systems have established vast data repositories that are largely inaccessible to the public and vulnerable to breaches, misuse, and even complete loss. The concentration of control within these centralized entities—mainly large tech corporations—has led to a plethora of issues. These include frequent data breaches, the exploitation of personal information for profit, and the monopolization of user identities, data, and access, which often results in invasive advertising and unjust censorship. The inefficacies of these systems are not simply technical challenges; they represent a fundamental barrier to achieving a secure, open, and equitable digital ecosystem.

The maturation of decentralized technologies, particularly blockchain and related cryptographic advancements, has presented an opportunity to revisit and reshape the underpinnings of digital trust. Despite promises of enhancing security and user agency, the adoption and practical implementation of these technologies in facilitating more reliable interactions remains under-explored.

Intuition is motivated by the need to address the current dichotomy between trustless systems and trustful interactions, offering a compelling solution rooted in decentralization. The proposed solution aims to not only advance the technical conversation around data and identity verification but also to catalyze a broader shift in how digital interactions are facilitated and perceived. By examining the shortcomings of current systems and exploring the potential of decentralized solutions, we endeavor to contribute to a foundational change in the digital trust landscape—one that is more aligned with the ideals of user empowerment, data integrity, and open access. The ultimate goal is to lay the groundwork for a digital infrastructure that upholds the values of an increasingly interconnected world, where trust is not a commodity to be controlled but a communal resource to be shared.

1.2 The Evolution of Digital Trust

Digital trust has undergone a profound transformation from the early days of the internet to the complex structures we encounter today. Whether it's connecting to the internet, downloading and installing new software, navigating to a URL, purchasing a product, or enabling machine-to-machine communication, almost every action in the digital realm requires placing trust in someone or something.

Initially, trust in the digital realm was a direct extension of real-world interactions, relying heavily on existing social structures and institutional assurances. Early internet users trusted based on familiar brands, personal recommendations, and institutional endorsements. As the internet expanded, digital trust began to encompass a broader array of signals, from email encryption protocols to the verification of websites through SSL certificates, laying the foundation for secure digital communications.

The dot-com boom and the rise of e-commerce platforms necessitated a new layer of trust mechanisms. These were often constructed on user reviews and ratings, third-party endorsements, and the burgeoning field of digital certificates. This era saw the emergence of trust intermediaries, such as certification authorities, which played a crucial role in authenticating the digital identities of websites and ensuring secure transactions.

The advent of social media further complicated the trust landscape by introducing peer networks as validators of content and character, blurring the lines between personal and platform-generated reputations. Platforms like Facebook and Twitter shifted the trust paradigm by making peer validation a core component of their systems, where likes, shares, and comments became indicators of credibility and influence.

With the emergence of Web2, companies started consolidating user data, creating comprehensive profiles to personalize experiences and, more lucratively, to target advertising. Trust became a byproduct of data and its associated analytics, with platforms and algorithms determining the reliability of information based on user interactions and engagement metrics. This model, while efficient, created a nexus of power around the oftentimes-opaque tech platforms, raising concerns about privacy and the ethical use of this data. These concerns led to a trust deficit between users and platforms, further exacerbated by frequent platform misappropriation of this newfound power, including data breaches and misuse scandals.

Archived copy · cryp2nova.com

The current phase in the evolution of digital trust is marked by the rise of decentralization, significantly driven by blockchain technology and related adjacent innovations. This movement heralds a return to principles of global, permissionless cooperation, user sovereignty, and transparency. This paradigm shifts power from intermediary platforms back to individuals, creating a trust architecture distributed across an ecosystem. In this model, permissionless, opt-in mechanisms ensure the integrity and authenticity of data.

The Ethereum blockchain, in particular, brought mainstream the concept of smart contracts, which enable developers to write and run code in a Turing-complete environment with unassailable, programmatic trust. This means developers can create arbitrarily complex and customized applications that run exactly as programmed without any possibility of downtime, censorship, fraud, or third-party interference.

This environment allows users to interact with arbitrarily complex code with nearly 100% programmatic trust guarantees. This near-certain programmatic trust is often referred to as 'trustlessness'. For instance, a smart contract for a decentralized financial application can automatically execute transactions, manage investments, or distribute profits based on predefined rules, without users of the application needing to rely on any central authority to maintain the integrity of the flow. This creates the first "trustless environment for arbitrarily-complex digital things," where trust is no longer a variable needing to be frequently considered, allowing users to "verify, not trust." Similarly to how we do not consider 'trust in the continued application of the laws of physics' when calculating gravitational forces, the 'immutable' rules of decentralized systems provide predictable outcomes, effectively removing trust from the equation and making interactions nearly as dependable as those natural laws.

Yet, as this paper explores, the present state of 'trustless code' is merely one, albeit crucial, element of the decentralized web and its fundamental migration towards objective trust systems. Revolutionary innovations such as trustless consensus, execution, and storage provide powerful assurances about the state of the system, but they do not fully address the broader spectrum of trust issues.

When viewed holistically, the decentralized web is still built, and still runs, on human-driven social consensus. Despite the advancements in trustless technology, the ecosystem relies on people to develop, maintain, and interact with these systems. Social consensus determines which projects gain traction, which protocols and proposals are adopted, how conflicts are resolved, etc. This human element introduces subjectivity and the potential for manipulation, making the decentralized web susceptible to many of the same pitfalls of the centralized systems it seeks to disrupt, such as centralization of power, security vulnerabilities, and trust deficits.

These layers of the trust stack cannot and should not yet be made completely 'trustless', and must instead be made 'trustful'. Take, for example, the Ethereum EIP process. In this scenario, rough social consensus is essential because decision-making in the decentralized realm is far too multi-variate of a problem to be handled purely programmatically. On-chain governance through token holder votes often exposes the complexity of such decisions, revealing pure codification of these types of processes as more of a bug than a feature. Decisions that require nuance, context, and human judgment cannot be effectively reduced to simple yes/no votes or algorithmic determinations (yet). While on-chain mechanisms can provide a governance framework, they fall short in capturing the full range of considerations needed for effective decision-making. Therefore, we must continue to rely on subjective social consensus and cannot yet make every layer of the decentralized web 'trustless'. We can, however, build technology to make these layers increasingly 'trust**ful**'.

Intuition acknowledges that digital trust is not static but an ever-evolving construct that must adapt to the changing contours of technology, society, and individual expectations. As we advance, it is crucial to blend technological innovation with human-centric design to foster genuine trust and collaboration in the digital age. This involves not only improving the underlying protocols and systems but also addressing the social and psychological aspects of trust. Understanding this evolution is crucial for developing systems that can foster genuine trust and collaboration in the digital age. By leveraging both the strengths of decentralized technologies and the insights from social dynamics, Intuition aims to create a more resilient and trustworthy digital ecosystem.

1.3 Objectives and Contributions of the Whitepaper

The principal objective of this whitepaper is to articulate a comprehensive understanding of the current challenges in digital trust, and to introduce the Intuition protocol as a novel solution. By dissecting the complex dynamics of existing trust mechanisms and the burgeoning decentralized alternatives, this paper aims to highlight the pivotal role of trust in the modern digital ecosystem, the urgent need for reform, and a potential path forward in the form of Intuition.

Archived copy · cryp2nova.com

Primary Objectives:

- **Diagnose the Current Trust Paradigm**: To scrutinize the status quo of digital trust, particularly within centralized Web2 platforms, and to elucidate the limitations and risks inherent in these systems, such as data silos, privacy breaches, and the monopolization of data.
- **Examine Decentralization as an Alternative**: To explore the potential of decentralized technologies, including blockchain and distributed ledgers, in mitigating the identified issues of the current trust paradigm, starting with an examination of existing efforts and solutions and their associated strengths and weaknesses.
- **Propose the Intuition Protocol**: To present Intuition as an innovative approach that integrates the strengths of decentralized identity, data, and finance to foster a more resilient and user-centric model of digital trust.

In sum, this whitepaper contributes to the discourse on digital trust by offering a holistic view of the current challenges, an exposition of a decentralized solution, and a vision for a future where trust is a shared and verifiable commodity, underpinning the interactions within our digital society.

2 Background and Context

2.1 Trust

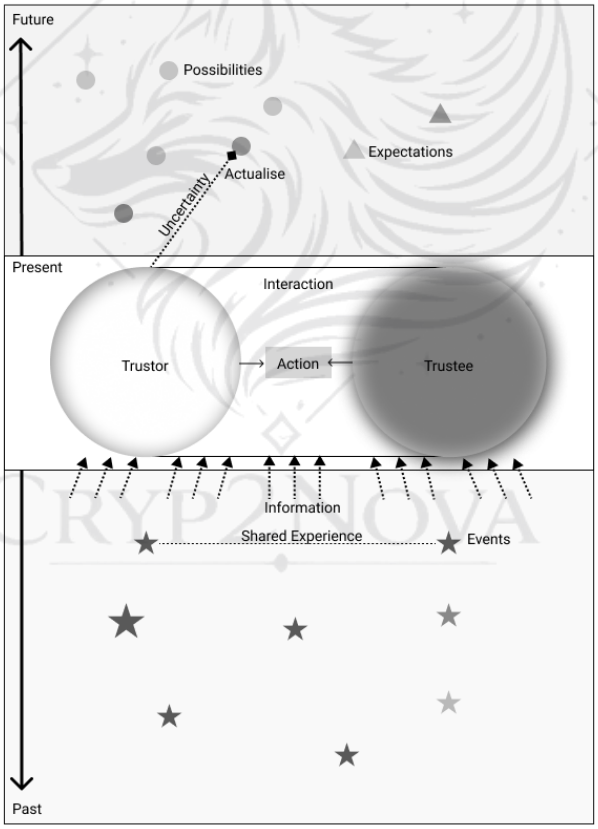


Figure 1: Dr. Will Abramson, 'Placing Trust', https://iiexhibition.studio/exhibit/6

The establishment of trust is a nuanced process, intricately woven into the fabric of human interaction. Trust permeates our daily lives, influencing decisions ranging from the products we purchase, to the relationships we cultivate, to the things we believe. But how do we navigate this landscape of trust? How do we discern what and whom to trust, and by extension, determine what to engage with, and how?

Archived copy · cryp2nova.com

Trust is fundamentally constructed on subjective experiences, reasoning, and intersubjective consensus, reinforced by familiarity, credibility, observability, and reliability. We rely on past experiences, personal relationships, and societal norms to assess the trustworthiness of individuals, institutions, concepts, and entities. These evaluations are not made arbitrarily but are informed by the continuous aggregation of data over time. For instance, when selecting a healthcare provider, we might consider recommendations from friends, the reputation of the medical facility, and the credentials of the healthcare professional. Each of these factors serves as a data point that shapes our overall trust assessment.

Moreover, trust is also influenced by contextual factors such as cultural norms, social cues, and the dynamics of specific situations. In uncertain or ambiguous circumstances, we often seek reassurance from trusted sources or rely on our intuition, which itself is shaped by accumulated data from our experiences, observations, and social learning.

Beyond human interactions, our understanding of most fundamental principles is rooted in trust, grounded in data and consensus. For example, in mathematics, we trust that the sum of two numbers will always yield the same result because of the consistency of the underlying natural phenomenon and because we, as a society, have agreed upon the symbols and rules that describe the phenomenon. Similarly, we gain trust in cryptographic systems through repeated validation of underlying algorithms and a social consensus on the standards and protocols used to implement and describe these systems.

In physics, our trust in the laws of motion and gravity is built on extensive observation and experimentation, as well as a shared understanding and description of the principles that describe these phenomena. For instance, we continue to trust Isaac Newton's laws of motion and universal gravitation, formulated centuries ago, as they continue to hold true and are consistently validated through experiments and practical applications, from predicting planetary orbits to engineering stable structures. This trust is reinforced by consensus on the scientific methods and principles used to describe and predict physical phenomena.

Additionally, because most people do not have the time, resources, or expertise to independently verify all of the complex ideas and principles they encounter, most 'trust' is inescapably rooted in a reliance on the consensus of knowledgeable authorities. This reasoning consists of higher-order derivates of lower-level trust, established through intersubjective consensus rather than direct observation, evidence, and introspection. This reliance on trusted parties as 'trust anchors' is especially crucial in areas like distributed systems and cryptography, where the underlying mathematics can be highly complex. Similarly, in processes such as government-issued identification, like passports, we rely on the government as a trust anchor. Instead of personally verifying cryptographic methods or bureaucratic processes, individuals place their trust in the consensus of experts who have rigorously tested and validated these systems.

In essence, every factor that influences our decisions can be viewed as a form of data. Whether it's the reputation of a brand, the advice of peers, or a gut feeling in a particular situation, each piece of information contributes to our understanding and trust. The process of establishing trust is, therefore, one of continuous data interpretation, where we analyze, synthesize, and contextualize available, relevant, and interpretable information to make informed decisions.

As we navigate the complexities of human interactions and the natural world, our capacity to discern trust and make informed decisions is crucial. This ability underpins our social fabric, enabling cooperation, collaboration, and mutual exchange. Trust, built on a foundation of reliable data, consistent observation, and social consensus, allows us to engage confidently with the world around us.

2.2 Identity

Every entity and concept - be it a person, an organization, a word, a product, a restaurant, a mathematical concept, etc. - has an identity, which serves as a conceptual anchor to which we attach and correlate data, experiences, and perceptions. 'Identities' also serve as a conceptual anchor where intersubjective data, experiences, and perceptions can commingle and converge. With this, identities act as the organizing principle that brings structure and context to data, transforming it from an undifferentiated sea of information into a comprehensible and actionable resource.

This foundational concept is crucial for establishing trust. Trusting an entity requires clear differentiation from other entities and a sufficiently-comprehensive dataset about it. As such, in pursuit of trust, a core focus must be on the identity of "things" and the development of systems that simplify how users intuit the nature and intentions of those things.

Archived copy · cryp2nova.com

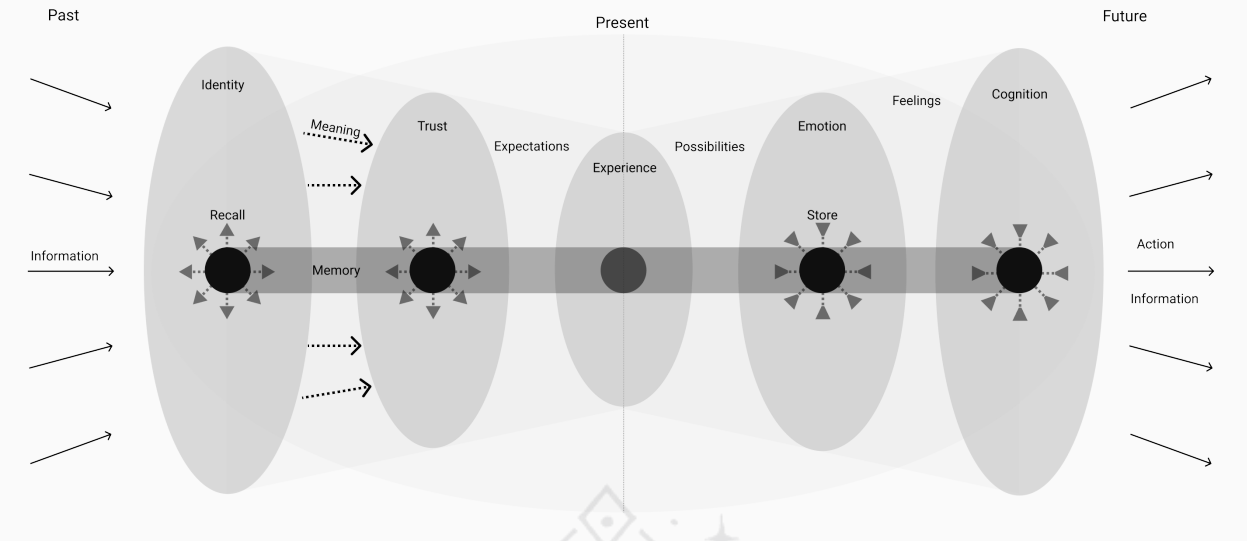


Figure 2: Dr. Will Abramson, 'Experience', https://iiexhibition.studio/exhibit/2

To conceptualize the concept of identity, the 'true identity' of an entity may be thought of as the 'Form' in Plato's Theory of Forms, representing the universal qualities that define it. From this philosophical concept, we derive, create, nurture, and evolve practical, relative, and contextual 'identities' that serve as our avatars - to ourselves and to others - as we navigate an increasingly-interconnected world. For example, a person's true nature may differ significantly from a digital 'identity' they curate for themselves, and to represent themselves, on platforms like Instagram, LinkedIn, or Twitter. Consequently, the identity models constructed by people and platforms observing and attempting to understand that person are not holistic, much like fragmented rays of light passing through a prism.

These models, though simplified and reductive, are constructed from available data to help interpret an entity's nature and role. The richness and effectiveness of our interactions with any entity directly correlate with the depth and breadth of data we possess about it. For example, understanding a person's historical reliability can enhance trust and facilitate smoother transactions, while familiarity with a device's functionalities can lead to more intuitive usage.

However, it is important to acknowledge that most identity models are imperfect representations of the true nature or identity of the entity, constrained by the available data. A few interactions with a person, for example, cannot fully encapsulate their true identity. Yet, often, such limited data is all we have to inform our judgments and assumptions.

The digital revolution has significantly expanded the scope of available identity data. Platforms such as social media have increased access to personal information, while IoT devices and online services provide detailed data about objects and their usage, weaving a more interconnected societal fabric. This enhanced data availability has enabled the construction of more detailed identity models, improving our ability to understand and engage within society.

Despite these advances, digital identities remain fragmented and reliant on the platforms that create and store this data. Moreover, a significant amount of identity-related data remains unexpressed, preventing a comprehensive portrayal of our true selves in the digital realm. This fragmentation limits our ability to form a holistic understanding of entities, and in turn, to interact with these entities successfully. The move towards a more unified and open approach to identity data could revolutionize how we interact with the world around us. By expanding and refining the data we collect and improving how we model identity, Intuition aims to provide a more accurate, trustworthy, and intuitive experience in all of our interactions.

2.3 Trust & Identity in the Digital Realm

The intersection of identity, data, and trust in the digital realm reveals a nuanced and evolving landscape. While core principles of trust remain consistent, the environment for establishing and maintaining trust has

Archived copy · cryp2nova.com

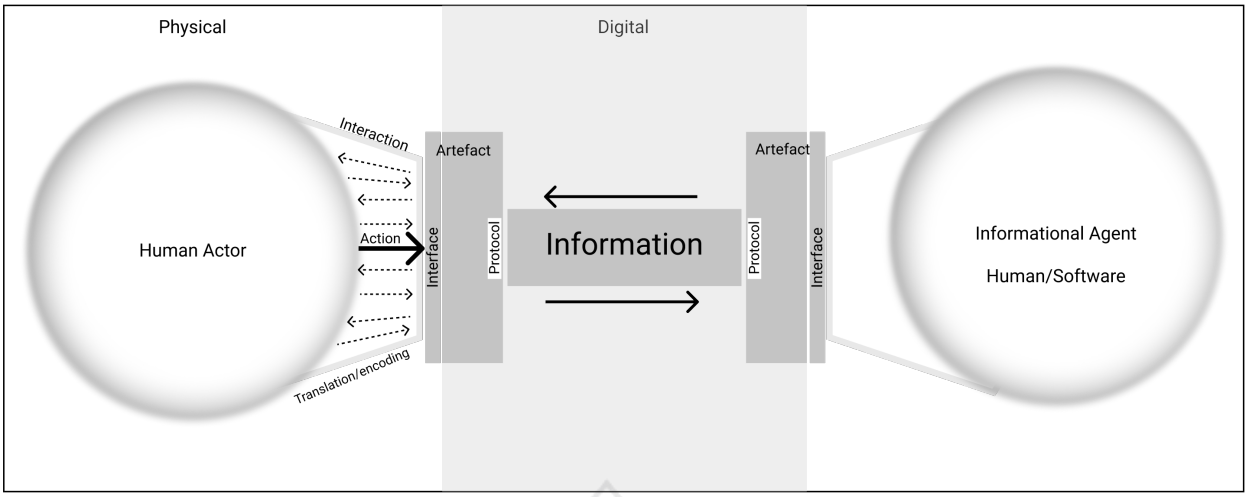


Figure 3: Dr. Will Abramson, 'Digital Mediation', https://iiexhibition.studio/exhibit/10

transformed dramatically. Data has emerged as the primary currency of trust, fundamentally reshaping interactions, transactions, and relationships in unprecedented ways.

The digital ecosystem is a vast network of interconnected platforms, services, and networks, each generating and processing immense volumes of data. This data, ranging from user-generated content and transactional records to behavioral analytics and algorithmic insights, forms the foundation of digital trust. Unlike traditional settings where trust is built through direct, tangible interactions, the digital world relies heavily on digital signals and data flows to mediate trust.

Trust in the digital domain is multifaceted, incorporating both explicit and implicit elements. Explicit trust mechanisms, such as user reviews, ratings, certifications, and cryptographic proofs, provide clearly-interpretable indicators of reliability and quality, helping users navigate the expansive digital bazaar. Implicit trust, on the other hand, is built indirectly through experiences and interactions. It emerges subtly through social connections, network effects, and algorithmic recommendations, developing gradually as users observe consistent and reliable behavior over time. Together, these explicit and implicit elements construct a comprehensive framework of digital trust, enhancing confidence and credibility in an intrinsically decentralized and distributed environment.

However, this new terrain is not without its challenges. The anonymity and pseudonymity that digital platforms often offer can sometimes shield malicious activities, creating opportunities for misuse and deception. Additionally, the rapid evolution of technology and data-driven algorithms can inadvertently introduce biases and distortions, which may erode trust and exacerbate inequalities across digital platforms.

To counter these vulnerabilities, a range of initiatives aimed at bolstering digital trust has emerged. These include decentralized identity systems, cryptographic safeguards, and technologies that enhance transparency and data governance frameworks. Additionally, community-driven approaches like community notes and prediction markets have gained traction as methods to reinforce trust by leveraging collective intelligence and consensus. These efforts are designed to give individuals greater control over their digital identities and data, enhance transparency and accountability in transactions, and address the asymmetries that can undermine trust and integrity in digital interactions.

Navigating this complex digital landscape requires a concerted effort to foster trust and ensure integrity in all interactions. By harnessing data-driven insights, embracing technological advancements, and advocating for collaborative governance, we can build a digital ecosystem that not only empowers individuals but also supports widespread innovation and serves the greater good. This vision guides Intuition as it strives to enable a more interconnected and trustworthy digital future.

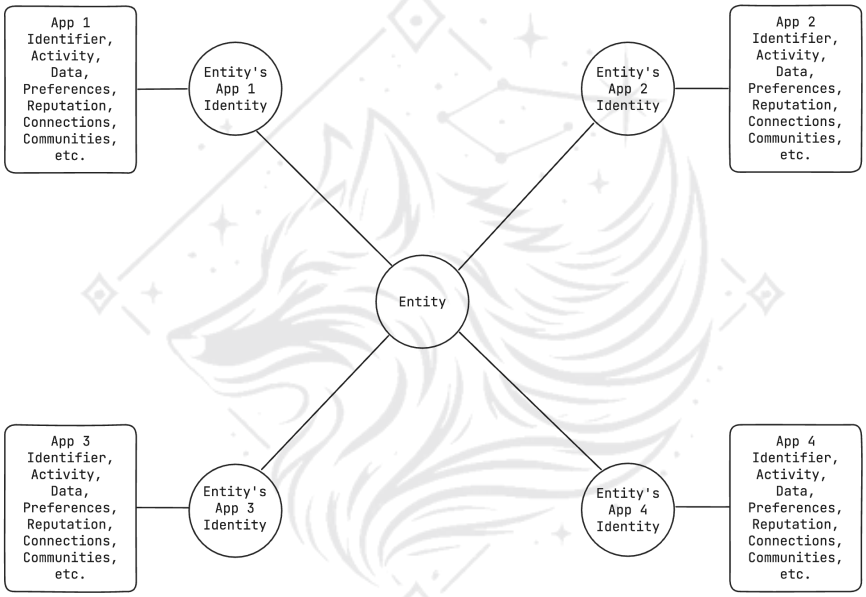
Archived copy · cryp2nova.com

2.4 The Contemporary Landscape of Digital Identity and Trust Mechanisms

As the digital landscape continues to evolve, 'identity' persists as a preeminent connector, linking individuals, entities, concepts, and their myriad interactions within the digital sphere. Each interaction we engage in—be it through social media profiles, website domains, or cryptographic keys—is layered with identity-related data that molds and defines the dynamics of trust. This data acts as a gateway through which we access, analyze, and interpret information, making identity a crucial component in establishing and maintaining trust.

As the nature of data and its applications continue to evolve, our identity systems must also adapt. The digital environment is becoming more intricate and interconnected, necessitating identity frameworks that can handle increased complexity and provide more nuanced representations of trust. This means developing systems that can integrate diverse data sources, manage dynamic identity attributes, and ensure privacy and security while facilitating seamless interactions for all.

2.4.1 Application-Specific Identity



In the early days of the internet, digital identities were rudimentary, often represented merely by user/hostnames or email addresses. These basic identifiers sufficed for the limited interactions of the time, with trust built on direct knowledge of interacting parties and institutional validation. This simplistic model of trust was intuitive and easily comprehensible to early internet users.

However, as the internet expanded in scale and complexity, the need for more sophisticated identity management and trust mechanisms became apparent. The growth of e-commerce, social networking, and a myriad of online services necessitated intricate systems for managing digital identities, especially for entities beyond people. Detailed profiles, reputation metrics, and trust scores emerged, allowing users to create multifaceted profiles for themselves, their enterprises, or their products. These profiles, intertwined with reputation metrics, became central to the online experience, facilitating a wide range of activities from social engagement to commercial transactions.

Trust in this advanced digital landscape evolved into a tapestry woven from user-generated content—spanning reviews, ratings, social media engagements, and more—combined with algorithmically-driven insights. Platforms aggregated vast amounts of data, analyzing user behavior to generate trust ratings and recommendations. This data-driven approach revolutionized trust establishment, leveraging vast datasets to provide users with invaluable insights and assurances for their online interactions.

However, the proliferation of application-specific identity introduced several challenges. Firstly, this paradigm inherently leads to a fragmented user experience. The compartmentalization of identities and associated data hinders the seamless transfer of preferences, communities, connections, reputation, and more

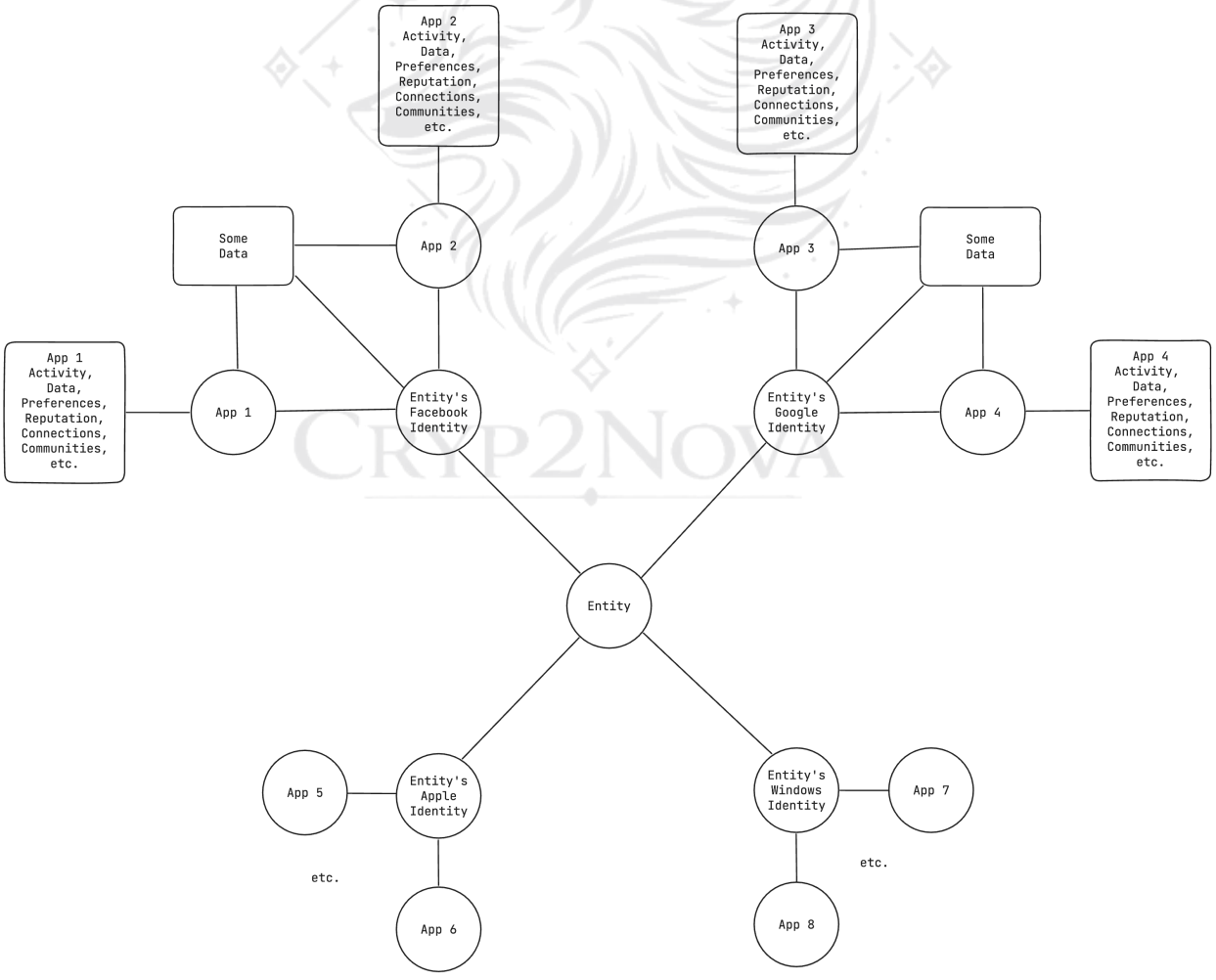
Archived copy · cryp2nova.com

across different digital environments. Users are required to manage separate credentials and data profiles for each platform they interacted with, forcing them to recreate digital personas and rebuild data histories from scratch with each new platform they joined, resulting in a disjointed online experience.

The application-specific identity model also imposes a heavy burden on developers, requiring them to not only build and maintain their own data and identity management systems but also to focus on accumulating vast amounts of user data. This approach significantly complicates the development process, diverting valuable resources and attention away from the team's core competencies and product innovation. Instead of concentrating on what makes their product unique, developers are compelled to address the challenges of identity and data management. For example, ensuring the protection of user data demands robust encryption, secure storage solutions, and regular security audits—tasks that often require specialized cybersecurity expertise. However, with cybersecurity talent in short supply, many development teams struggle to implement these measures effectively, leading to increased vulnerabilities and potential security breaches.

Moreover, the fragmentation of identities and data across incompatible, isolated silos—reminiscent of the disconnected early tribes of humanity—complicates the establishment of trust and adds considerable friction to the processes of understanding and decision-making. This highlights the pressing need for more integrated and interoperable identity and data management solutions. A unified system would allow for the seamless transfer of credentials, preferences, reviews, reputations, recommendations, and data across different digital platforms, resulting in a more cohesive, user-centric, and efficient digital experience.

2.4.2 Federated Identity



Archived copy · cryp2nova.com

Federated identity systems emerged as a response to the inefficiencies and fragmentation inherent in application-specific identities. These systems aim to create a more integrated and interoperable approach to identity management across the digital landscape. By enabling users to access multiple platforms and services with a single set of credentials, federated identity systems significantly simplify the digital experience. Prominent examples include 'Sign in with Google' or 'Sign in with Facebook,' which offer streamlined authentication processes across various web environments.

By adopting standardized protocols such as Security Assertion Markup Language (SAML) and OpenID Connect (OIDC), federated identity systems centralize identity management functions. This centralization bolsters security and enhances user convenience, significantly improving the overall user experience by eliminating the need for multiple logins. Such efficiency mitigates the risks associated with password reuse and potential credential theft, saving users from the cumbersome task of managing numerous passwords. Additionally, for platform developers, federated identity systems abstract away the complexities of authentication and credential management. This means platforms do not need to become experts in security practices, as these functions are handled by the federated identity provider. This allows developers to focus on core features and innovations rather than investing significant resources into maintaining secure authentication systems.

An additional key benefit of federated identity systems is their potential to enable the seamless transfer of personal preferences, community connections, and other elements of a user's digital identity across various platforms, by providing cross-platform unique identifier(s) representative of the user around which data can be aggregated. This interoperability has the potential to foster a more unified and cohesive online presence, allowing users to maintain relatively consistent identities and carry over their settings, networks, and preferences to any new platform they join. This continuity is crucial for enhancing user engagement and loyalty by providing more personalized and relevant digital interactions across a spectrum of services. However, as evidenced by the current web experience, this potential remains largely underexplored.

At its core, federated identity demonstrates a better way to build trust within the digital ecosystem. It enables the possibility of more transparent and accountable representations of users' identities across different platforms. By offering a consistent and reliable identity verification method, these systems allow users to engage confidently across diverse services, knowing that their digital persona is both recognized and trusted. This reinforced trust is crucial, not only enhancing security but also deepening the relationships between users, platforms, and service providers, thus paving the way for more secure, reliable, and meaningful interactions in the digital world.

Yet, despite these advancements, significant issues remain. Federated identity systems centralize control and trust into the hands of a few major tech companies like Google and Facebook, potentially compromising user privacy and autonomy. This centralization stands in stark contrast to the principles of decentralization, concentrating power and control for the sake of convenience. Such centralization risks include potential misuse of user data, single points of failure, and heightened vulnerability to large-scale breaches. Additionally, the internet remains fragmented, with many services operating in isolation and leading to data silos where user information is confined within specific applications. While federated identity systems provide some infrastructure for data portability and interoperability, critical gaps persist, and the promise of a truly seamless digital experience remains largely aspirational.

Federated Identity Trust Assumptions Enhancing the discussion of federated identity, it's critical to delve into the underlying trust assumptions that govern this system. As mentioned, while federated identity systems offer significant benefits in terms of interoperability and ease of use, they oftentimes require users and platforms to place a considerable degree of trust in a central identity provider, such as Google or Facebook, when using Single Sign-On (SSO) services.

This trust is multifaceted and built upon several layers:

1. **Trust in the Provider's Security Practices:** Users must trust that the identity provider implements robust security measures to protect their identity and credentials from breaches and unauthorized access. The assumption here is that the provider is capable of safeguarding sensitive data better than the individual platforms could independently.
2. **Trust in the Provider's Integrity:** There is an inherent trust that the identity provider will not misuse the identity data they manage. This includes trusting that the provider will not exploit the data for unintended purposes, such as surveillance, selling data to third parties, or manipulating services to the detriment of the user.

Archived copy · cryp2nova.com

3. **Trust in the Provider's Continuity:** Users and platforms depend on the continuous operation and reliability of the identity provider. This trust entails the expectation that the provider will maintain their services without interruption and will not suddenly revoke access or shut down a service without adequate notice, which could leave users stranded without access to multiple accounts.
4. **Trust in the Provider's Compliance:** There is also a trust that the provider complies with relevant laws and regulations, particularly concerning data protection and privacy. This compliance is crucial not only for protecting individual rights but also for ensuring that the services do not become liabilities due to legal shortcomings.
5. **Trust in Platform Interoperability:** Lastly, users trust that the identity provider will maintain compatibility and interoperability with various platforms. This includes updating and adapting their services in line with evolving technological standards and security practices, ensuring that the federated identity system remains practical and secure over time.

These trust layers form a comprehensive 'trust stack' that users implicitly accept when they opt to use centralized federated identity systems. While these systems simplify and secure access to multiple services, they also centralize risk and control to a significant extent. Recognizing these trust assumptions is essential for users and platforms alike to make informed decisions about their participation in federated identity systems and to understand the potential vulnerabilities and dependencies these systems introduce into the digital identity landscape.

2.5 The Current Web2 Trust Stack

Having explored the evolution from application-specific identities to federated identity systems, it's crucial to understand how these paradigms shape the current Web2 trust stack more generally. This foundation allows us to appreciate the existing mechanisms and their inherent flaws, setting the stage for why a transition to decentralized models is necessary.

2.5.1 A Typical Web2 Interaction

To understand the current Web2 trust stack, consider a common scenario: purchasing a product on Amazon. The process involves several steps and trust assumptions:

1. **Account Creation and Login**:
   - Users create an account on Amazon.
   - **Trust Assumption**:
     - Users trust Amazon to handle their personal information securely and provide accurate authentication.
     - Users trust that Amazon will allow the user to sign up for and authenticate to the platform.
2. **Product Search and Selection**:
   - Users search for products, relying on Amazon's search algorithm to display relevant results.
   - **Trust Assumption**:
     - Users trust that Amazon's algorithms accurately rank products based on quality, relevance, and user reviews.
3. **Review and Rating Analysis**:
   - Users read product reviews and ratings to gauge product quality and seller reliability.
   - **Trust Assumption**:
     - Users trust that reviews are genuine and not manipulated by sellers or competitors. They also trust the platform's moderation systems to filter out fake or misleading reviews.
4. **Payment and Checkout**:
   - Users enter payment information and complete the purchase.
   - **Trust Assumption**:
     - Users trust Amazon's payment processing system to handle their financial information securely and protect them from fraud.
5. **Order Fulfillment and Delivery**:

Archived copy · cryp2nova.com

- Users wait for their product to be delivered, relying on Amazon's logistics network.
- **Trust Assumption**:
  - Users trust Amazon and its delivery partners to fulfill the order accurately and on time.

6. **Post-Purchase Support**:
   - Users may need to return products or seek customer support.
   - **Trust Assumption**:
     - Users trust Amazon's customer service to resolve issues fairly and efficiently.

2.5.2 Flaws in the Web2 Trust Stack

As framed through the example above, the centralized nature of Web2 platforms introduces several vulnerabilities and challenges:

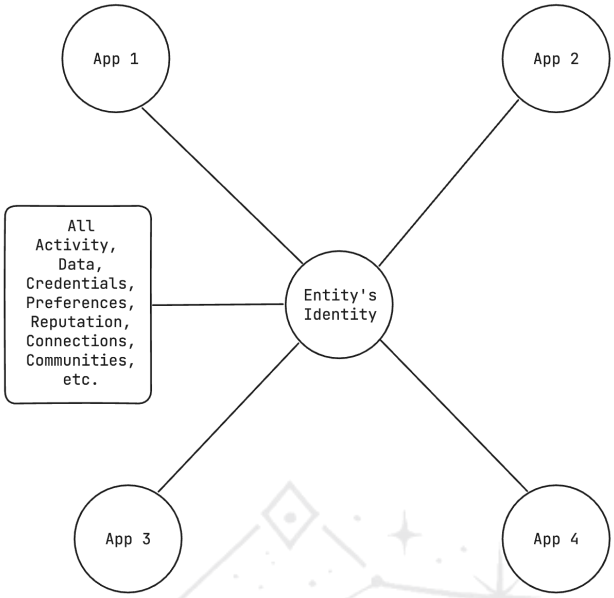
1. **Data Privacy and Security**:
   - Centralized platforms control vast amounts of user and user-generated data, making them prime targets for data breaches and misuse. Users have little control over how their data is stored, shared, or sold.
2. **Algorithmic Transparency**:
   - Algorithms that govern search results, recommendations, and review moderation lack transparency. Users cannot verify if these algorithms are fair or biased, leading to potential manipulation.
3. **Monopolistic Control**:
   - A few dominant platforms hold significant power, limiting competition and innovation. Users are often locked into ecosystems with little recourse if they are dissatisfied with the service.
4. **Review Manipulation**:
   - The reliability of reviews and ratings can be compromised by fake reviews, paid promotions, or biased moderation. Users cannot easily discern the authenticity of the information they rely on.
5. **Single Points of Failure**:
   - Centralized systems are vulnerable to outages, cyberattacks, and policy changes. Users are at the mercy of the platform's stability and integrity.
6. **Erosion of User Trust**:
   - Repeated data breaches, privacy scandals, and opaque practices have eroded user trust in centralized platforms. Users are increasingly concerned about their data privacy and the fairness of digital interactions.

As we can see, though these systems offer convenience, they also concentrate power and control, exposing users to a plethora of risks. As we transition to Web3, addressing these flaws by decentralizing trust and empowering users with greater control over their digital identities and interactions becomes imperative.

2.6 The Role of Decentralization in Reshaping Digital Trust

Decentralized/decentralizing technologies are fundamentally reshaping how trust is established and maintained in the digital realm. These technologies aim to migrate the digital world from subjective trust systems, which rely on human judgment and intermediaries as outlined above, to objective trust systems, based on programmatic and mathematical proofs. Within this decentralization paradigm, the seamless user experience of familiar Web2 systems can be achieved - and even surpassed - with significantly fewer trust assumptions. With this comes a shifting of power to the edges of the system, distributing it away from the centralized control of institutional gatekeepers. As a result, control and data are redistributed back to individuals, democratizing access and participation. This shift not only creates a more secure and transparent framework for digital interactions but also redefines the mechanisms through which trust can be established and maintained.

Archived copy · cryp2nova.com



2.6.1 Decentralized Identity & Agent-Centric Data

The evolution from a federated identity model to a model of decentralized identity and agent-centric data represents a significant advancement in how we establish and maintain trust in digital interactions. Rooted in the idea that a unified set of self-sovereign credentials can be used to seamlessly interact with the entire web, this approach aggregates data around a single universal identifier for each agent in the system. This paradigm shift eliminates the need for intermediary identity providers and gatekeepers, thereby facilitating more seamless interoperability across the web. By removing the explicit need to trust specific centralized entities for identity and data management, decentralized identity and agent-centric data fosters a more trustful digital environment.

Importantly, this model does not suggest a uniform identity for all interactions. Instead, it supports a system where multiple contextual identities (e.g., professional, personal) are anchored to a central identifier and associated set of credentials. Advanced cryptographic techniques ensure the privacy and distinctiveness of these identities while maintaining user control. This structure allows the maintenance of distinct personas tailored to different contexts while benefiting from the coherence and continuity provided by a unified identity framework.

The concept of decentralized identity also extends beyond individuals to encompass all entities—products, services, concepts, and more. By adopting the same decentralized identity patterns used for individuals and assigning globally persistent decentralized identifiers to all entities, data aggregation can similarly center around these universal identifiers rather than disparate, application-specific ones. This approach helps obviate the need for extensive data reconciliation efforts across platforms. For example, product reviews could be seamlessly aggregated from across the entire internet, rather than being scattered across various centralized platforms, akin to Tim Berners-Lee's vision of the Semantic Web. The interoperability afforded by these universal identifiers helps to ensure that data associated with any entity is consistently and coherently managed, enhancing the overall efficiency and utility of digital interactions.

In the realm of blockchain technology, decentralized identifiers are already prevalent, with Ethereum addresses serving as a prime example. An Ethereum address functions as a decentralized identifier due to its unique, verifiable nature and independence from intermediaries. Importantly, Ethereum externally owned accounts (EOAs) are based on secp256k1 elliptic-curve-derived keys. This cryptographic standard ensures secure and interoperable transactions across the entire Ethereum ecosystem, eliminating the need for intermediaries. Consequently, users do not need to create separate accounts for each application; a single Ethereum address operates as a unified, decentralized identifier, enabling streamlined and secure interactions across the ecosystem.

Furthermore, the cryptographic principles underlying Ethereum addresses extend their utility beyond the Ethereum network. The secp256k1 elliptic-curve-derived keys, which form the basis of Ethereum EOAs, are

Archived copy · cryp2nova.com

widely recognized and supported across various blockchain and cryptographic systems. This compatibility allows Ethereum keys to be utilized for authentication and secure transactions in other environments that adopt the same cryptographic standards.

Ethereum addresses are also not limited to representing users, as smart contracts also have addresses. This characteristic extends the concept of decentralized identifiers to non-human entities, enabling the aggregation of agent-centric data around these addresses. Consequently, both users and smart contracts can interact within the same ecosystem, using a unified system of identifiers. This agent-centric approach fosters more efficient data management and interoperability, as data associated with a particular address—whether it belongs to a user or a smart contract—can be more seamlessly aggregated and utilized across different platforms and applications.

2.6.2 Public Key Infrastructure (PKI) Proliferation

One often overlooked yet transformative benefit of blockchain-based systems is their significant contribution to advancing Public Key Infrastructure (PKI). Blockchain technology has compelled millions of users to manage their own private keys, thereby reclaiming control over their digital identities. This shift is crucial for the next evolution of the internet—one that minimizes many of the trust assumptions inherent in Web2. As the blockchain ecosystem necessitates the interaction with and management of cryptographic keys, numerous teams have developed sophisticated technologies to assist users in handling self-sovereign identifiers. What was once a complex and cumbersome process is becoming increasingly accessible and user-friendly, thanks to the innovations driven by the blockchain community.

With this ease of use comes the feasibility of additional utility. Public Key Infrastructure (PKI) has long been a cornerstone of digital security, providing the framework for encrypting, signing, and verifying data. Historically, PKI was primarily used for secure email, SSL/TLS for web traffic, and VPNs. However, the advent of blockchain technology has significantly broadened the adoption and utility of PKI. With the rise of blockchain wallets, millions of users now possess self-sovereign private keys. The widespread proliferation of blockchain wallets has democratized access to robust cryptographic tools, empowering users to engage in secure, trustless interactions across decentralized networks. Today, PKI underpins a wide range of decentralized systems, enabling essential security functions that ensure the integrity and authenticity of digital interactions:

- **Cryptographic Authentication**
  - PKI enables cryptographic authentication, ensuring that only the legitimate owner of a private key can initiate transactions or access certain data. This authentication is foundational to maintaining trust in decentralized systems, where traditional intermediaries are absent.
- **Data Integrity**
  - By using digital signatures, PKI ensures that data has not been tampered with. Every transaction or message signed with a private key can be verified by others using the corresponding public key, guaranteeing that the data remains intact and unaltered.
- **Non-Repudiation**
  - PKI provides non-repudiation, ensuring that a user cannot deny the validity of their signed transactions. This feature is crucial for accountability in decentralized systems, where trust must be established without centralized oversight.
- **Decentralized Identity**
  - PKI is integral to the development of decentralized identifiers (DIDs) and verifiable credentials (VCs), explored in more detail later in this paper. These technologies rely on PKI to enable self-sovereign identity management, allowing users to control their identity information and share it securely across different platforms.
- **Secure Communication**
  - PKI facilitates secure communication between participants in decentralized networks. By encrypting messages with the recipient's public key, users can ensure that their communications are private and secure from eavesdropping or interception.
- **Interoperability**

Archived copy · cryp2nova.com

– The standardized nature of PKI allows it to function across various platforms and blockchain networks. This interoperability is critical for creating a cohesive and interconnected decentralized ecosystem, where trust can be maintained consistently across different services and applications.

2.6.3 Building Trustless Systems with Blockchain Technology

Decentralized identifiers (DIDs) have commenced a revolution in establishing and maintaining digital trust by bestowing users with sovereignty over their identities, eliminating dependency on intermediaries. Nonetheless, DIDs alone are insufficient to entirely escape the trust assumptions entrenched in the Web2 stack. To actualize a genuinely trustless internet, it is imperative to have platforms where these DIDs can be employed securely and directly. This necessity is fulfilled by decentralized applications (dApps).

With the advent of blockchain technology, a movement is underway to mitigate the reliance on traditional trust assumptions prevalent in Web2. Blockchain platforms, notably Ethereum, are at the forefront of this paradigm shift, enabling the construction of trustless systems wherein interactions are governed by transparent and immutable code, thereby obviating the need for intermediaries.

The Ethereum ecosystem has been pioneering in the development of dApps through smart contracts—self-executing agreements that operate precisely as programmed without susceptibility to censorship or interference. These smart contract platforms act as "decentralized world computers," enabling users to use decentralized identifiers to permissionlessly engage with arbitrarily complex code distributed across a network of nodes.

This transition from subjective trust systems, reliant on intermediaries, to objective trust systems, governed by transparent and immutable code, constitutes a fundamental shift in digital trust. It eliminates the need to place trust in third parties, allowing users to 'verify, not trust.' Understanding how this shift is possible requires an exploration of the core objective-trust mechanisms within the decentralized web stack, which are currently laying the foundation for a more secure and reliable digital future:

Consensus Consensus mechanisms are the cornerstone of decentralized networks, enabling a global, distributed, and permissionless network of participants to maintain the integrity of the 'world computers.' These mechanisms ensure that all honest nodes agree on the blockchain's state, even in the presence of malicious actors. In blockchain ecosystems, consensus mechanisms secure the network by requiring validators to commit significant resources. In Proof of Work (PoW) systems, computational power is used, while in Proof of Stake (PoS) systems, validators stake tokens. This resource commitment makes it prohibitively expensive for attackers to manipulate the system, thereby safeguarding the network's integrity.

The consensus process is inherently transparent and verifiable, with every state transition recorded on a public ledger accessible to anyone. This transparency fosters trust by allowing independent verification of the blockchain's integrity and the validity of transactions. The distributed nature of consensus mechanisms ensures that no single entity has control over the network, aligning with the core principles of decentralization.

Execution Once a network can reach distributed consensus, the next logical step is to determine the applications for which this consensus can be applied. The concept of a 'world computer' where anyone can code arbitrarily complex logic becomes feasible, enabling the use of distributed consensus for a myriad of applications. This is epitomized in the trustless execution layer of the decentralized web's stack.

Trustless execution, primarily facilitated by smart contracts, is a fundamental component of decentralized systems. These self-executing programs on blockchains like Ethereum automate state transitions based on predefined conditions, without intermediaries, ensuring that their terms will be enforced exactly as written. Every state transition is recorded on the blockchain, ensuring a transparent and auditable history.

Storage Trustless storage is a critical enhancement to the trust stack, providing secure and reliable data storage through decentralized networks. This ensures data accessibility and security without reliance on central authorities, which is particularly vital for applications requiring long-term data integrity, such as record-keeping and decentralized applications.

Decentralized storage is an intrinsic feature of all blockchain systems. Blockchains inherently function as decentralized storage solutions because they require a distributed ledger that all participants can access and verify. Every transaction and state transition on a blockchain is recorded in a decentralized manner, ensuring data integrity and availability across the network.

Archived copy · cryp2nova.com

In addition to the storage provided by blockchains themselves, there are specialized decentralized storage solutions such as IPFS, Filecoin, and Arweave. These technologies extend the concept of decentralized storage beyond the blockchain, distributing data across a network of nodes. This distribution ensures that the data is not reliant on a single point of failure, enhancing its robustness and resilience. By eliminating the need for a central provider, decentralized storage addresses issues like censorship and data loss risks. Data replication across multiple nodes ensures redundancy and availability, even if some nodes fail.

Cryptographic techniques can secure the data, ensuring that only authorized parties have access despite it being widely distributed. Once data is signed and stored in these systems, it cannot be altered, providing a reliable and immutable record of its history. This immutability is crucial for applications that depend on the long-term integrity and verifiability of data.

By leveraging both blockchain-based and specialized decentralized storage solutions, the decentralized web can ensure a high level of data integrity and accessibility. This decentralized approach to storage underpins the trustless systems that are essential for the next evolution of the internet, supporting a wide range of applications and ensuring that data remains secure and available without centralized oversight.

Economic Incentives Trustless economic incentives are fundamental to the functioning of decentralized systems, enabling trustless consensus, execution, and storage. These incentives drive the participation of individuals and entities in maintaining and securing decentralized networks, ensuring their integrity and reliability without the need for central authorities.

In decentralized networks, consensus mechanisms such as Proof of Work (PoW) and Proof of Stake (PoS) rely heavily on economic incentives to encourage participants to act in the network's best interests. In PoW systems, miners expend computational resources to solve cryptographic puzzles, with the successful miner receiving a block reward and transaction fees. This process not only secures the network by making it costly for malicious actors to attack but also incentivizes honest behavior through potential financial gains. Similarly, in PoS systems, validators lock up a certain amount of cryptocurrency as a stake. They are selected to validate transactions and create new blocks based on the size of their stake and other factors. Honest validators earn rewards in the form of additional tokens, while dishonest behavior can result in the loss of their staked tokens. This alignment of economic interests with network security ensures robust protection against attacks and promotes the overall health of the network.

Trustless execution is also supported by economic incentives. Smart contracts, which automate the execution of agreements on the blockchain, often include mechanisms to reward participants who contribute to their successful execution. For instance, decentralized finance (DeFi) platforms use smart contracts to facilitate lending, borrowing, and trading of assets. Users are incentivized to provide liquidity, execute trades, or participate in governance by receiving economic rewards such as interest, fees, or governance tokens. These incentives ensure active participation and the smooth functioning of decentralized applications.

Decentralized storage networks leverage economic incentives to ensure data integrity and availability. In systems like IPFS, Filecoin, and Arweave, participants are rewarded for contributing storage resources and maintaining data over time. For example, in Filecoin, storage providers earn FIL tokens for storing and retrieving data. The economic model encourages providers to offer reliable and secure storage services, as their financial rewards depend on their performance and reputation within the network. This incentivization model creates a robust and resilient storage system that is decentralized and free from single points of failure.

The relationship between trustless economic incentives and decentralized systems is intrinsically symbiotic. While trustless consensus, execution, and storage are reliant on trustless economic incentives, these mechanisms are conversely necessary for the creation, upkeep, and transaction of trustless economic rewards. These mechanisms enable the existence and transaction of 'provably scarce digital assets' for the first time in history, allowing decentralized assets to maintain significant economic value, as exemplified by cryptocurrencies like Bitcoin and Ether. Without these mechanisms, the properties that make these assets valuable would be compromised, reducing the incentives for participation.

When viewed holistically, these foundational elements—decentralized identifiers, PKI proliferation, trustless consensus, trustless execution, trustless storage, and trustless economic incentives—enable society to transition towards increasingly objective trust systems. However, as the rest of this paper will outline, building a comprehensive trust stack necessitates addressing a broader scope of issues. The following sections will

Archived copy · cryp2nova.com

delve into how Intuition aims to solve these challenges, creating a robust and resilient framework for the decentralized web.

2.6.4 The Role of Social Consensus in Blockchain Systems

A critical aspect not often mentioned in discussions about trustless systems is the role of social consensus. In the blockchain world, nearly everything, including the 'trustless' consensus mechanisms, ultimately relies on social consensus. At its core, even the most decentralized blockchain systems depend on the collective agreement of their participants.

Consensus Mechanisms and Social Trust Consensus mechanisms, such as Proof of Work (PoW) and Proof of Stake (PoS), are foundational to blockchain security. These mechanisms enable decentralized networks to agree on the state of the blockchain without relying on a central authority. However, the effectiveness of these mechanisms hinges on the collective behavior and integrity of the network participants. Miners and validators must act in the best interest of the network, and the community must reach a social consensus on which blockchain protocol to follow and which upgrades to implement.

For example, Bitcoin and Ethereum, the two largest blockchain networks, are secured by PoW and PoS respectively. Their resilience and security are testaments to the robustness of these consensus mechanisms. Despite being constantly attacked and scrutinized, they have maintained their integrity and uptime, showcasing the power of decentralized consensus. However, this resilience is also a result of the social consensus among the community of developers, miners, validators, and users who collectively work to uphold and improve the network.

Intersubjective Fault Tolerance Intersubjectivity refers to the shared understanding and agreement among multiple individuals, and can be likened to social consensus. It plays a crucial role in our daily lives as it forms the basis of social interactions, collective decision-making, and consensus building. Unlike purely objective facts that can be independently verified, intersubjective agreements depend on the collective perceptions, beliefs, and judgments of people.

Eigenlayer's introduction of the intersubjective work token, EIGEN, represents a significant advancement in recognizing the limitations of purely deterministic and cryptographic verification systems. While the blockchain conversation has largely been focused on the development of trustless, objective mechanisms (which are still, to some extent, reliant on social consensus, as outlined above), the EIGEN whitepaper acknowledges that numerous tasks and decisions require human judgment and social consensus.

EIGEN highlights the critical role of social consensus in the decentralized web, emphasizing that many systems cannot be entirely 'trustless'. Instead, they require broad-based agreement among participants. This shift from purely objective verification to incorporating human judgment is essential for handling complex, context-dependent scenarios that cannot be reduced to algorithmic determinations.

Social Consensus Beyond Technical Protocols The concept of social consensus extends beyond the confines of technical protocols and permeates society at large. In everyday life, intersubjective faults—errors in judgment due to misunderstandings, biases, or insufficient information—are commonplace. These errors occur because our decisions are shaped by subjective perspectives, social interactions, and the lack of high-quality, relevant, and interpretable data. To address these faults, systems need to be developed that not only prevent them but also enhance society's ability to tolerate and manage them when they do occur.

The need for fault-preventative intersubjective consensus is particularly critical in the context of the decentralized web, where it significantly influences decisions and interactions, and where poor decisions can lead to catastrophic consequences. Choices regarding which platforms to use, which decentralized applications (dApps) to trust, which protocol upgrades to implement, and which information sources to rely on are typically influenced by collective social agreements, informed heavily by social cues, endorsements, and reputations.

For instance, the popularity and trustworthiness of a decentralized application are often established more through community endorsements and social proof than through purely technical merits. Influencers, developers, and early adopters play pivotal roles in building trust and driving adoption. Therefore, users must place a significant degree of trust in these individuals and communities, despite the decentralized web's foundational aim to minimize the need for trust. This reliance highlights the importance of developing robust systems that can support and enhance social consensus, ensuring that collective decision-making in the decentralized web is as reliable and informed as possible.

Archived copy · cryp2nova.com

2.7 Trustless Code vs Trustful Interaction

As we can see, the promise of a decentralized web is enticing, but the reality of interacting within this ecosystem can still be daunting and fraught with risk. Despite the maturation of the foundational layers of trustless technology, users continue to face significant challenges and trust assumptions when navigating Web3.

For example - a typical user's journey in Web3 begins with setting up and managing a wallet. This process involves several trust assumptions, such as ensuring the software installation is from a legitimate source, securely storing private keys or seed phrases, and trusting the integrity of the wallet software. Risks such as phishing, human error, and software vulnerabilities pose significant threats. Fake wallet applications and websites can steal users' private keys, while misplacing a seed phrase or falling victim to social engineering attacks can result in the loss of all assets. Additionally, vulnerabilities in wallet software can be exploited by hackers to steal funds, underscoring the necessity for users to trust the software developers and their security practices.

When interacting with decentralized applications (dApps), users must trust the security of smart contracts and the respective chain(s) they live on, navigate to the correct URLs, and rely on the integrity of oracles that fetch off-chain data. The risks include, but are not limited to, smart contract exploits, phishing attacks, and oracle manipulation. Bugs or vulnerabilities in smart contracts can lead to significant financial losses, while users can be tricked into interacting with fake dApps designed to steal their funds. Malicious or faulty oracles can provide incorrect data, leading to unintended consequences in smart contract execution.

Navigating ecosystem information adds another layer of complexity. Users rely on information from various sources, such as social media, forums, and influencers, to make informed decisions. They must trust the accuracy of this information, the validity of reviews and endorsements, and the reliability of reputation systems. Misinformation, review manipulation, and reputation abuse can mislead users, resulting in poor decision-making and potential losses.

With this, despite the trustless infrastructure provided by blockchain technology, users must still place significant trust in **people**. Expecting every user to meticulously read and understand every line of code and every concept they interact with is unrealistic and impractical. Instead, users must trust that developers have written secure and reliable code and rely on the intersubjective consensus of their trusted communities to vet the things they interact with. This reliance on human trust means that, for the foreseeable future, the decentralized web must still be underpinned by traditional subjective trust mechanisms.

2.8 The Trust Paradox of 'Trustless' Systems

As exemplified, despite the advancements in decentralized platforms aimed at reshaping digital trust, a paradox remains at the core of these systems: while decentralized technologies strive to transition the world away from subjective trust systems and towards more 'objective' trust systems (AKA 'trustless' systems), the decentralized web still fundamentally relies on human behaviors and decision-making. Paradoxically, because the lower levels of the stack are trustless, we often require much stronger subjective trust—since if something goes wrong, the results can be catastrophic, with no method for reversing transactions or paths to recourse. This inherent paradox creates a nuanced and complex trust landscape that remains largely unaddressed.

Although the promise of these technologies is to enable direct peer-to-peer interactions, theoretically eliminating the need for third-party intermediaries, the reality is more complex. The effective functioning of these platforms still heavily relies on human factors, including the integrity of developers, the behavior of network participants, and the community's ability to reach consensus on key issues.

This interplay between technology and human elements highlights the limitations of achieving a fully trustless environment. While Web3 technologies enable the migration to less subjective trust systems, they do not completely eradicate the necessity for trust. Users still need to trust that they are interacting with the 'right' things, that smart contracts are coded correctly, that oracles provide accurate data, that the community will act in the network's best interest, and so forth.

As such, achieving a more 'trustful' stack is a complex endeavor that requires innovative solutions to navigate the intricate challenges of establishing and maintaining digital trust in a decentralized environment.

Archived copy · cryp2nova.com

2.9 The Trustful Interaction Layer

To address the limitations and complexities identified in achieving a trustful decentralized environment, Intuition's primary focus is the conceptualization and implementation of a 'trust**ful** interaction layer'. While the trustless backbone of decentralized systems provides a robust foundation, these alone are insufficient for creating a secure and user-friendly ecosystem. The current landscape still presents significant challenges in ensuring trustful interactions for users navigating Web3. Therefore, the next step involves developing a trustful interaction layer that addresses these issues more comprehensively.

This trustful interaction layer seeks to bridge the gap between trustless protocols and the practical needs of users by combining the strengths of decentralized technologies with mechanisms that enhance user trust and safety. By integrating trust-enhancing features and facilitating more informed interactions, we can create a decentralized environment that not only preserves the core principles of Web3 but also ensures a more reliable and secure user experience.

2.9.1 The Spectrum of Approaches

To effectively construct a trustful interaction layer, it is essential to examine the spectrum of potential approaches, ranging from entirely centralized to entirely decentralized systems.

Centralized Gatekeepers: The Extreme of Centralization At one extreme of the spectrum lies the entirely centralized approach, reminiscent of the early days of the internet and exemplified by platforms like AOL. In this model, centralized gatekeepers exert significant control over the ecosystem, dictating who and what users can interact with. This approach offers a curated and controlled user experience, theoretically ensuring security and trust by filtering out malicious actors and content. However, it comes with severe drawbacks:

- **Centralized Power**: Gatekeepers hold disproportionate power, potentially leading to censorship, data monopolies, and abuse of authority. This concentration of control is antithetical to the decentralization ethos, where power is distributed to avoid single points of failure and abuse.
- **Single Points of Failure**: Centralized systems are vulnerable to attacks and failures, risking the security and accessibility of user data.
- **User Disempowerment**: Users have limited control over their interactions and data, conflicting with the fundamental principles of decentralization.

This centralized model, while offering some degree of security and trust, stands in stark contrast to the values of the decentralized web, which aims to empower users and distribute control.

Wisdom of the Crowds: The Extreme of Decentralization At the opposite end of the spectrum is the entirely decentralized approach, relying on the collective wisdom of the crowds. In this model, decisions and trust are established through widespread social interactions and user-generated content. This approach includes:

- **Personal Interactions:** Engaging with peers directly, especially over calls, at conferences, and at events, to gather insights and recommendations. This method leverages personal trust networks but lacks scalability and can be geographically and temporally limited.
- **Social Media and Online Platforms:** Scrolling through platforms like Twitter, Reddit, and others to gauge sentiment and gather opinions. While democratizing information dissemination, these platforms are rife with misinformation, echo chambers, and manipulation.
- **User Reviews and Ratings:** Utilizing platforms like Yelp, Amazon, and Google Reviews to make informed decisions based on collective user feedback. Although useful, these reviews can be biased, manipulated, or overwhelmed by low-quality content.

While this approach aligns with the ethos of decentralization and empowers individuals, it also has significant limitations:

- **Information Overload:** Users are inundated with vast amounts of unstructured data, making it difficult to extract meaningful insights. The sheer volume of information can overwhelm users, leading to decision fatigue and analysis paralysis.

Archived copy · cryp2nova.com

- **Misinformation and Bias:** User-generated content can be manipulated, biased, or inaccurate, leading to poor decision-making. The lack of verification mechanisms can result in the spread of false information, undermining trust.
- **Lack of Structure:** The decentralized nature of this approach lacks the necessary structure to efficiently filter and validate information. Without a coherent framework, it is challenging to establish reliable and consistent trust metrics.

Finding Balance Building a trustful interaction layer requires a nuanced approach that transcends the binary choice between centralization and decentralization. By integrating the strengths of both models, we can create a system that is secure, user-friendly, and aligned with the core values of the decentralized web. This balanced approach will pave the way for a more robust and trustworthy digital ecosystem, enabling users to navigate Web3 with confidence and ease.

2.9.2 The Role of Identity, Data, and Incentives in Creating a Trustful Interaction Layer



Figure 4: The DIKW Pyramid, https://en.wikipedia.org/wiki/DIKW_pyramid

In exploring our solutions to the Trust Paradox, our solution must fundamentally revolve around the intricate relationship between identity and data. In earlier sections, we explored how trust is established through data and its interpretation, and how identities serve as conceptual anchors for accumulating and correlating this data. To create a truly trustful interaction layer, we must bring these concepts full circle, recognizing that many of the challenges we face in the digital realm are essentially problems of identity and data management.

Trust, both in the physical and digital worlds, is built upon familiarity, credibility, and reliability. In the digital realm, where direct interactions are replaced by data flows and digital signals, the need for reliable identity models and comprehensive data becomes even more critical. These identity models, though imperfect, help us navigate the complexities of the digital ecosystem by providing a framework for understanding the entities we interact with.

In this framework, identities must extend beyond personal identification to encompass organizations, smart contracts, products, and even concepts. Each of these requires a robust identity model that can be anchored in verifiable data. This data, whether it comes from user-generated content, transactional records, or behavioral analytics, forms the backbone of trust in the digital landscape. The more data we have about an entity, the clearer our understanding and the higher our trust in that entity.

Therefore, to create a 'trustful interaction layer', the focus must be on building technologies and systems that can continuously gather, validate, and present relevant data in a transparent and accessible manner. Intuition aims to address these challenges by providing a robust system for identity and data refinement, expression, and management - giving entities better 'intuition' in all of their interactions.

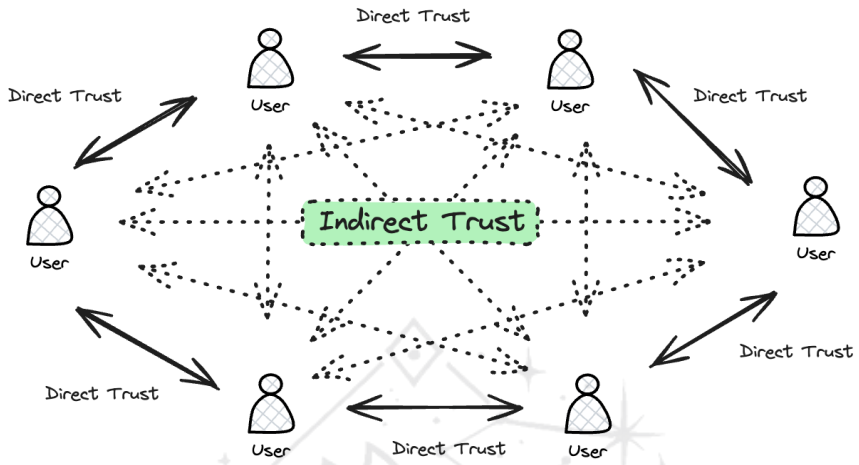
3 Current Solutions

In pursuit of a trustful interaction layer, leveraging and building upon the foundational work of numerous innovators and technologists is essential. Intuition is constructed on these existing solutions, and by examining them, we can better appreciate the landscape of tools and protocols that Intuition leverages and enhances.

Archived copy · cryp2nova.com

Here, we explore key concepts, offerings, and advancements that can be leveraged in the development of a holistic trust stack, from identity verification to data validation mechanisms.

3.1 The Web of Trust



When examining the intersection of identity and data, the 'Web of Trust' emerges as a pivotal concept, encompassing a range of ideas that remain relevant across various contexts. The core principles of a Web of Trust provide a framework for understanding how trust can be established and maintained in decentralized systems.

The Web of Trust concept originated in the early 1990s as a decentralized model for public key authentication, primarily used in PGP (Pretty Good Privacy) encryption. Unlike traditional hierarchical systems where a central authority validates identities, the Web of Trust allows individuals to vouch for each other's public keys. This decentralized approach to trust management ensures that no single entity has control, promoting a more resilient and user-empowered network.

Expanding this concept to a broader range of interactions, in a Web of Trust, individuals and entities build trust through direct interactions and endorsements within a network. Each participant functions as a node, forming connections grounded in mutual trust. These connections create a distributed trust network where reputation is established through social validation rather than centralized authority. The decentralized nature of this network aligns with the ethos of Web3, empowering users to control and manage their own trust relationships.

To ensure the reliability of endorsements, a Web of Trust typically employs verifiable claims and attestations. Participants sign their endorsements with private keys, creating cryptographic proofs of authenticity. These verifiable claims can be audited and traced back to their origin, adding a layer of accountability and transparency. This mechanism mitigates the risk of misinformation and manipulation, ensuring that trust is based on verifiable data.

3.2 Identity and credential verification

Identity and credential verification are foundational to establishing trust in both centralized and decentralized systems. These processes involve not only confirming that individuals or entities are who they claim to be, but also validating the authenticity of their credentials and assessing their trustworthiness and reputation. This is crucial for nearly every interaction in society - ranging from opening bank accounts, accessing government services, or entering establishments with age limits (such as a liquor-serving bar), to making informed decisions about hiring someone for a job, verifying university degrees, buying authentic products, and ensuring the integrity of transactions.

3.2.1 Centralized Identity and Credential Verification

In centralized systems, identity verification typically relies on authoritative entities such as government agencies and major service providers. These entities issue credentials like passports, driver's licenses, and

Archived copy · cryp2nova.com

diplomas, which are used to authenticate individuals and authorize transactions. However, centralized systems come with significant drawbacks, including security vulnerabilities, privacy concerns, and the risk of power abuse. Centralized databases are prime targets for hackers, and breaches can result in the exposure of sensitive personal information. Additionally, individuals have limited control over their digital identities, relying on central authorities to manage and protect their data. This centralization creates single points of failure and can lead to exclusion and discrimination, particularly for individuals who do not have access to required documentation or are marginalized by the system.

3.2.2 Decentralized Identity and Credential Verification

In contrast, decentralized identity solutions aim to return control of personal data to individuals. Leveraging core cryptographic principles, these solutions create secure, self-sovereign identities that can address both quantitative and qualitative verification needs. At the core of the off-chain decentralized identity ecosystem are the specifications developed by the **World Wide Web Consortium (W3C)**. The W3C's work on **Decentralized Identifiers (DIDs)** and **Verifiable Credentials (VCs)** has been instrumental in shaping the decentralized identity landscape.



Figure 5: Simple example of a decentralized identifier, https://www.w3.org/TR/did-core/

Decentralized Identifiers As mentioned earlier, decentralized identifiers serve as an ideal fulcrum point for aggregating data. DIDs are a modern type of identifier that enable verifiable, self-sovereign digital identities. Unlike traditional identifiers such as email addresses or usernames, DIDs are not tied to a centralized registry, identity provider, or certificate authority. Instead, they are created, owned, and managed by individuals themselves. Each DID document contains the public keys and service endpoints necessary to authenticate the DID owner and facilitate secure interactions. The W3C DID specification provides a standardized framework for creating and using DIDs across different platforms and services, ensuring interoperability and fostering a cohesive ecosystem where users can seamlessly manage their identities.

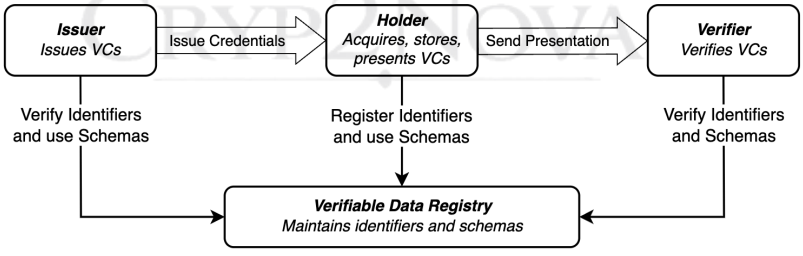


Figure 6: The roles and information flows forming the basis for the W3C VC specification, https://www.w3.org/TR/vc-data-model-2.0/

Verifiable Credentials (VCs) VCs are cryptographically secure credentials that individuals can present to verify their identity or claims. These credentials are typically issued by trusted entities and can be independently verified without the need for a centralized intermediary. VCs can encapsulate a wide range of information, from university degrees and professional certifications to personal attributes like age and nationality. The W3C VC specification outlines how credentials can be formatted, issued, and verified in a decentralized manner, ensuring interoperability across various platforms and enabling users to present their credentials to multiple verifiers with confidence in their authenticity and integrity.

Archived copy · cryp2nova.com

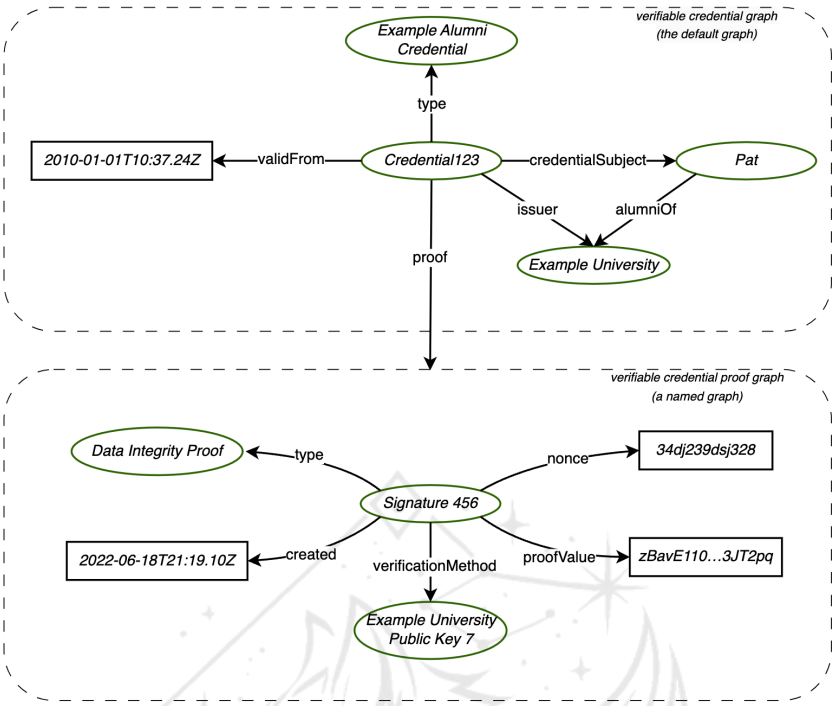


Figure 7: Information graphs associated with a basic verifiable credential, https://www.w3.org/TR/vc-data-model-2.0/

3.2.3 Benefits of Existing Decentralized Identity Solutions

Decentralized identity solutions offer several significant advantages over centralized systems. Individuals have full control over their digital identities, deciding when and how their personal information is shared. Decentralized systems reduce the risk of large-scale data breaches, as personal information is not stored in a central repository. Cryptographic principles ensure that data is securely transmitted and verified. DIDs and VCs are designed to be interoperable across different platforms and services, enabling seamless interactions in a decentralized web. Moreover, decentralized solutions can provide a richer context for trust assessments, with VCs including endorsements from peers, work performance reviews, or detailed educational records, allowing for a more comprehensive evaluation of an individual's trustworthiness and qualifications.

3.2.4 Requirements of Existing Decentralized Identity Solutions

Despite the promise of these technologies and their applicability to enhancing trust in our interactions, they have substantial requirements that must be addressed if they are to realize their full potential:

Secure and Efficient Storage Solutions One of the primary concerns in decentralized identity systems is the development of secure and efficient storage solutions for Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs). Off-chain storage needs to ensure data integrity, confidentiality, and availability. Unlike centralized systems, where data is stored in a single location and controlled by a central authority, decentralized systems distribute data across multiple nodes, increasing the complexity of data management.

1. **Data Integrity:** Ensuring that data remains unaltered and accurate over time is crucial. In decentralized systems, where multiple copies of data may exist, maintaining consistent and tamper-proof records is a significant challenge.
2. **Confidentiality:** Protecting sensitive information from unauthorized access is paramount. Decentralized systems must implement robust encryption and access control mechanisms to ensure that only authorized parties can view or modify data. This is particularly challenging when dealing with personally identifiable information (PII) or other sensitive data, which requires stringent privacy protections.

Archived copy · cryp2nova.com

3. **Availability:** Ensuring that data is accessible when needed, despite the decentralized nature of the storage, is essential. Decentralized storage solutions must provide high availability and fault tolerance, so users can access their identity information reliably. Technologies like InterPlanetary File System (IPFS) and Arweave offer decentralized data storage with built-in redundancy and availability, but integrating these solutions seamlessly into decentralized identity systems remains a complex task.

Interoperability Between Identity Providers Ensuring interoperability between different identity providers is essential for the decentralized identity ecosystem to function smoothly. The diverse range of platforms and services must communicate and understand each other's DIDs and VCs to enable seamless user experiences across multiple contexts.

Developing and adhering to common standards and protocols is critical for interoperability. The W3C's DID and VC specifications provide a foundational framework, but widespread adoption, consistent implementation across various platforms, and convergence on data schemas are still necessary. Without these common standards, users face friction when attempting to use their identities across multiple platforms, limiting the utility of decentralized identities.

Protocols for Issuing, Managing, and Verifying Credentials Creating secure, scalable, and user-friendly protocols for issuing, managing, and verifying credentials is another complex task. These protocols must facilitate the seamless creation and revocation of credentials, as well as provide mechanisms for users to manage their credentials effectively.

1. **Security:** Ensuring that the protocols are secure and resistant to attacks is paramount. This includes protecting against unauthorized issuance or revocation of credentials and ensuring the integrity and authenticity of the credentials themselves.
2. **Scalability:** The protocols must be able to handle a large number of users and transactions without becoming inefficient or overly costly. This is particularly important in decentralized systems, where network congestion and high transaction fees can pose significant challenges.
3. **User Experience:** The protocols must be designed with the end-user in mind, ensuring that they are easy to use and understand. Users should be able to manage their credentials without needing deep technical knowledge, and the processes for issuing and verifying credentials should be intuitive and straightforward.
4. **Standard Schemas**: There is a need for standardized schemas to ensure interoperability and consistency. Protocols must adopt and adhere to common data schemas, enabling seamless interaction and understanding between different platforms and services. This standardization is essential to prevent fragmentation and ensure that credentials can be universally recognized and verified.

Adoption Adoption is particularly vital for Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs) to achieve their full potential. Without broad adoption, the advantages of these inherently communal technologies cannot be fully utilized, which limits their impact and effectiveness and creates a chicken-and-egg dilemma.

- **Critical Mass of Users**: For DIDs and VCs to function effectively, a significant number of individuals, organizations, and institutions need to participate. A critical mass of users ensures that there are enough entities issuing, managing, and verifying credentials to create a robust and functional ecosystem. This widespread participation enhances the utility and reliability of decentralized identity solutions.
- **Interoperability**: Adoption by a diverse range of platforms and services is necessary to achieve true interoperability. When multiple stakeholders use standardized DIDs and VCs, it ensures seamless interaction and verification across different systems. This interoperability reduces friction for users and increases the overall effectiveness of decentralized identity solutions.
- **Trust Network Expansion**: The success of DIDs and VCs depends on a broad network of trusted issuers and verifiers. As more entities adopt these technologies, the trust network expands, making it easier for individuals to prove their identity and credentials across various contexts. This expansion is crucial for establishing a reliable and universally accepted system of digital identity.

Archived copy · cryp2nova.com

- **Market Confidence**: Adoption by major players in various industries, including finance, healthcare, education, and government, can significantly boost market confidence in DIDs and VCs. When reputable institutions integrate these technologies, it signals their reliability and security, encouraging more users to adopt them.
- **Policy and Regulation**: Government and regulatory bodies play a pivotal role in the adoption of DIDs and VCs. Clear policies and regulations that support the use of decentralized identities can provide the legal framework necessary for widespread adoption. Regulatory support can also address concerns related to security, privacy, and compliance, making it easier for organizations to integrate these technologies.
- **Education and Awareness**: Educating the public and organizations about the benefits and functionalities of DIDs and VCs is essential for driving adoption. Awareness campaigns, workshops, and training programs can help demystify these technologies and demonstrate their practical applications. Increased understanding leads to greater acceptance and use.
- **Infrastructure Development**: Building the necessary infrastructure to support DIDs and VCs is crucial for adoption. This includes developing user-friendly interfaces, secure storage solutions, and efficient protocols for issuing and verifying credentials. Investments in infrastructure ensure that decentralized identity solutions are accessible and practical for everyday use.
- **Community Engagement**: Engaging with the community of developers, businesses, and end-users is vital for fostering innovation and addressing challenges. Collaborative efforts can lead to the development of best practices, standards, and solutions that drive the adoption of DIDs and VCs. A supportive community also helps in addressing technical and regulatory hurdles.

Ultimately, widespread adoption is the major linchpin for realizing the full potential of DIDs and VCs. It requires a concerted effort from all stakeholders, including users, organizations, regulators, and developers, to create a thriving ecosystem that leverages the advantages of decentralized identity solutions.

3.3 Ethereum as a Decentralized Identity Platform

Recognizing it as a potential solution for many of the previously-mentioned requirements, some early decentralized identity experiments, such as ConsenSys's uPort, chose Ethereum as the platform for building decentralized identity / attestation / verifiable claim / Web of Trust offerings, with Ethereum's potential for identity and reputation systems even being highlighted as a key use case in Vitalik Buterin's original whitepaper. Ethereum solves for many of these requirements by providing several advantages, including a permissionless and decentralized ledger, widespread adoption, the ability to create programmatic value flows, and robust security guarantees. The use of self-sovereign private keys, cryptographic signatures, and timestamped data entries offers a strong foundation for secure and verifiable identity management, addressing many of the challenges in the decentralized identity ecosystem.

One of the earliest efforts was the drafting of EIP 725, which proposed Proxy Accounts. Proxy Accounts were designed to act as a proxy for individuals' identifiers. The concept emerged from the realization that leveraging a private key as an identifier poses several issues, particularly the inability to rotate keys if they are compromised. The solution was to create a singular proxy contract representing an individual, which could allow for key rotation. uPort was among the pioneers in developing these Proxy Accounts. They introduced some of the earliest social recovery mechanisms, allowing a pre-determined list of addresses to recover the wallet or change the controller of the proxy contract through a multi-signature method. This innovation addressed the vulnerability of losing access to the identity due to key loss or compromise.

Building on the Proxy Accounts, uPort introduced EIP 780, which proposed the Ethereum Claims Registry. This development aimed to enhance the trust and reliability of the identity system by enabling attestations. However, significant concerns arose regarding the architecture of these systems. The primary issue was the gas costs associated with deploying smart contract wallets for each new user and for every attestation. The cost of creating new accounts and recording attestations on-chain was prohibitive, especially considering the goal of extending financial and identity system access to underdeveloped and underprivileged regions.

To address the high gas costs, the uPort team developed the concept of metatransactions. These Ethereum transactions could be funded by a third party, allowing uPort to subsidize identity creation and attestations while keeping identifiers self-sovereign. Despite this innovation, the solution was not scalable. Subsidizing transactions for a growing user base proved to be impractical in the long term. However, metatransactions have since been open-sourced and have fostered a whole ecosystem, contributing to broader advancements in reducing transaction costs and improving accessibility in decentralized applications.

Archived copy · cryp2nova.com

In response to these scalability issues, uPort began leaning into an increasing amount of off-chain mechanisms. They introduced EIP 1056, known as "Lightweight Identity." This standard aimed to create and update identities with minimal use of blockchain resources. In EIP 1056, an identity could have an unlimited number of delegates and attributes, and identity creation was as simple as generating a regular key pair Ethereum account, incurring no gas costs.

Despite these advancements, concerns about identity correlation and social recovery mechanisms persisted. In the social recovery scheme, the addresses capable of recovering an identity were recorded on-chain, making them publicly available. This raised the risk that these addresses could be correlated with individuals, who could then be compromised to recover an identity on behalf of an attacker, effectively stealing the identity.

To mitigate these risks and others (especially around privacy and scalability), many identity projects began moving significant portions of their stack—or the entire stack itself—off-chain. This migration led Ethereum identity players to contribute to the broader off-chain decentralized identity ecosystem, inheriting the challenges of the decentralized identity ecosystem and significantly hindering adoption.

3.3.1 Renewed Interest in Ethereum as a Decentralized Identity Solution

Recent advancements in the Ethereum ecosystem have catalyzed a renewed interest in decentralized identity solutions, making it increasingly feasible to build these solutions on Ethereum.

Layer 2 scaling solutions, such as rollups, have significantly reduced transaction costs and increased throughput, enabling the storage and management of identifiers and data on-chain. As these Layer 2 solutions continue to drive gas costs towards zero, scalability concerns become less significant.

The introduction of smart contract wallets and account abstraction mechanisms, exemplified by EIPs 4337, 3074, and 7702, marks a significant leap forward in decentralized identity management. These innovations provide users with enhanced flexibility and security features essential for robust identity solutions.

EIP 4337 introduces account abstraction via a higher-level protocol, allowing users to leverage smart contracts for managing their accounts. This enables advanced functionalities such as multi-signature setups, meta-transactions, and automated recovery options, thereby enhancing the user experience and security of decentralized identity systems.

EIP 3074 focuses on allowing users to delegate control of their externally owned accounts (EOAs) to a contract, providing the ability for any EOA to act like a smart contract wallet without deploying a contract. This abstraction simplifies the user experience and reduces friction, making it easier for users to interact with decentralized identity systems.

EIP 7702 introduces enhancements to transaction management, enabling functionalities such as batching multiple operations, sponsorship where one account pays for another's transaction, and privilege de-escalation by allowing sub-keys with limited permissions. These features improve usability, security, and efficiency, making decentralized identity systems more user-friendly and versatile.

Sign In With Ethereum (SIWE) also represents a significant advancement in leveraging Ethereum addresses as decentralized identifiers, providing a secure and user-friendly authentication method. By allowing users to authenticate themselves using their Ethereum addresses, SIWE enhances the seamless integration of decentralized identity systems within the broader Web3 ecosystem. SIWE enables users to log into various platforms and applications using their Ethereum wallets, such as MetaMask. The process involves signing a unique authentication request with their private key, proving ownership of the Ethereum address without exposing sensitive information. This approach eliminates the need for traditional usernames and passwords, offering a more secure and streamlined user experience.

EIP-712, which standardizes the signing of structured data on Ethereum, can also be leveraged to solve the decentralized identity puzzle. EIP-712 introduces a structured and human-readable way to sign typed data, improving the security and usability of digital signatures. When users sign authentication requests or other transactions, they can see exactly what they are signing, reducing the risk of phishing attacks and accidental approvals of malicious transactions. This transparency is crucial for maintaining trust in decentralized interactions - for example, SIWE leverages EIP-712 to improve the user experience and security of the authentication process.

The Ethereum Name Service (ENS) has emerged as a cornerstone of decentralized identity on Ethereum, offering a user-friendly method for linking human-readable names to Ethereum addresses and other decentralized identifiers. ENS enables users to register names ending in .eth, which can then be used as a shorthand

Archived copy · cryp2nova.com

for Ethereum addresses, smart contracts, and even off-chain resources such as IPFS content. This greatly enhances the usability of decentralized systems by abstracting complex alphanumeric addresses into simple, memorable names.

The emergence of decentralized social networks like Lens Protocol and Farcaster marks a transformative change in the way social interactions and digital identities are handled on the blockchain. These platforms are at the forefront of developing decentralized social graphs, enabling users to fully own and control their social connections, personal data, and content. This ownership ensures that users can manage their digital presence without relying on centralized intermediaries, offering greater privacy and autonomy. The decentralized social graphs established by these platforms not only enhance user empowerment but also present valuable opportunities for integration with decentralized identity projects. By tapping into these networks, decentralized identity solutions can leverage the robust, user-controlled data structures created by Lens and Farcaster.

3.4 Attestations

The Ethereum ecosystem's recent advancements have significantly contributed to the development of an attestation ecosystem. Attestations are simply cryptographically signed statements made by entities about things. The cryptographic signing ensures these statements are verifiable and tamper-proof, which is essential for maintaining trust and integrity in decentralized identity systems. By leveraging Ethereum's decentralized infrastructure, attestations can be issued and verified without relying on central authorities.

Ethereum's ability to enable users and entities to issue and verify cryptographic attestations provides a robust framework for establishing trust and identity in a decentralized manner. Similar to Verifiable Claims or Credentials, attestations can represent a wide range of assertions, from simple claims about an entity's attributes to complex reputational data. This versatility allows for the creation of rich, multifaceted identity profiles.

Notable examples of the evolving attestation ecosystem include the Ethereum Attestation Service (EAS) and Verax. Both platforms offer scalable and decentralized solutions for issuing and verifying attestations. By leveraging the Ethereum blockchain, these services ensure that attestations are timestamped, secure, verifiable, and tamper-resistant, thus reinforcing the decentralized trust model.

These advancements empower us to easily and securely sign arbitrary data about various entities, creating verifiable evidence of who made a statement, what was said, and when it was said—all without the need for intermediaries. The implications of this development are profound, enabling a transformative shift in how trust and identity are managed in the digital realm. This marks a significant leap towards a more decentralized, transparent, and reliable internet, where trust is rooted in cryptographic proofs rather than centralized authorities. This shift not only enhances security and transparency but also democratizes digital interactions, paving the way for a truly decentralized web.

4 Current Challenges in Building a Trustful Interaction Layer

Despite advancements in trust-facilitating technologies such as decentralized identity and verifiable data solutions, the web's interaction layer still falls short of enabling efficient and well-informed decision-making. This gap can be attributed to several challenges, including those outlined below, which must be addressed in the pursuit of a reliable and effective digital ecosystem.

4.1 Identity Fragmentation

4.1.1 User Identity Fragmentation

Identity fragmentation persists in Web3, where individuals and entities often have multiple identifiers. This fragmentation leads to a lack of a unified digital persona, making the discernment of the reputation of any one identity difficult. In the Web2 world, users typically manage hundreds of accounts across various platforms, each with its own login credentials and identity attributes. This proliferation of identities is mirrored in Web3, where users might have multiple identifiers they use to interact across different blockchain networks and in different contexts.

Archived copy · cryp2nova.com

The primary issue with identity fragmentation is the challenge it poses for establishing a cohesive and comprehensive reputation. Each account or identifier may contain bits and pieces of a user's activities, interactions, and endorsements, but without a unified digital persona, it is difficult to aggregate this information into a coherent reputation profile. This disjointed nature of identities complicates trust and verification processes, as stakeholders must navigate through fragmented data to assess the credibility and reliability of an individual or entity.

Furthermore, managing multiple identities is cumbersome for users, leading to inefficiencies and potential security risks. Users may struggle to keep track of numerous credentials, increasing the likelihood of weak password usage, password reuse, and susceptibility to phishing attacks. In a decentralized context, the lack of a unified identity can hinder seamless interactions across platforms and services, reducing the overall user experience and slowing the adoption of decentralized technologies.

Recent advancements in the decentralized identity and blockchain wallet arenas are beginning to address these issues by allowing users to aggregate their identities and manage them as if they were one. However, challenges around identity correlation, interoperability, and consolidated reputation persist.

4.1.2 Non-User Identity Fragmentation

Identity fragmentation, typically discussed in the context of users, is equally critical for non-user entities such as products, services, and concepts. In the digital landscape, these entities often lack consistent and reliable identifiers, creating significant challenges in data aggregation, interoperability, and trust.

In the Web2 environment, non-user entities are identified through platform-specific identifiers, which are isolated and independently managed. This isolation prevents a unified and comprehensive view of any given entity, complicating efforts to establish and verify reputations, track provenance, and ensure data integrity. Each platform may maintain its own version of an entity's identity, leading to inconsistencies and duplication.

The emergence of decentralized identifiers (DIDs) offers a robust solution to this issue. DIDs provide a universal, persistent, and verifiable method to identify non-user entities across multiple platforms and contexts. By assigning DIDs to these entities, it is possible to create a cohesive digital representation recognized and trusted across different systems.

Unlike user identities, non-user entities, such as words or concepts, typically cannot possess self-sovereign identities due to their non-autonomous nature. Thus, there are two approaches to managing the sovereignty of these identities: they are either controlled by no one or collectively managed by a representative group (or everyone). The latter approach, facilitated by blockchain technology, introduces decentralized, community-governed identifiers.

Blockchains enable a paradigm in which the control over the identity of non-user entities can be decentralized and transparent. This approach allows the identity of a product, service, or concept to be managed through decentralized autonomous organizations (DAOs). These 'identity DAOs' or 'data DAOs' could help ensure the accuracy, consistency, and tamper-proof nature of identity information by relying on community consensus rather than a single centralized entity.

For instance, a decentralized dictionary managed by a 'data DAO' would revolutionize the way words and concepts are defined and maintained. Unlike traditional dictionaries, which are controlled by centralized entities such as Merriam-Webster, a data DAO leverages decentralized governance, ensuring that no single group has monopolistic control over language definitions. This decentralized approach democratizes the process of defining words, allowing contributions and consensus from a broad and diverse community. This participatory model fosters transparency and inclusivity, capturing the evolving nature of language more accurately.

Decentralized governance mechanisms within a data DAO also enable a more comprehensive and unified digital representation of concepts. As a result, data aggregation and interoperability may be significantly improved. The decentralized dictionary could seamlessly integrate with various applications, platforms, and services, providing a reliable and consistent source of information that is universally recognized. This approach not only enhances the reliability of digital data but also encourages continuous improvement and adaptation through community involvement, making it a more robust and dynamic system. However, due to the absence of innovation and experimentation in this area, the issue of non-user identity fragmentation remains.

Archived copy · cryp2nova.com

4.2 Data Expression, Availability, Fragmentation, Discoverability, and Comprehensibility

4.2.1 Lack of Expression

The current state of digital ecosystems, both Web2 and Web3, illustrates a pervasive issue: the mere presence of infrastructure for creating "claims about things" does not guarantee active user engagement and expression. This challenge is not confined to Web3; it is also evident in Web2 environments. For instance, platforms such as Yelp, Amazon, and Google provide robust systems for user reviews, yet the majority of users seldom participate. Similarly, professional networking sites like LinkedIn feature endorsement mechanisms that remain significantly underutilized, with only a small fraction of users actively endorsing their peers.

A significant volume of potentially valuable data remains untapped due to the lack of incentives for users to express this information. Without adequate financial, functional, or reputational rewards, users are less motivated to contribute meaningful data. Consequently, the digital landscape is often incomplete and less informative.

Specifically in the context of the decentralized web, the data necessary for successful interaction and navigation exists, but is frequently confined to the minds of individuals. Many users possess the knowledge required for effective decision-making within this environment, but this expertise typically stems from extensive time, attention, research, and active participation in specialized communities. There is a substantial gap in knowledge transfer from those who have mastered the ecosystem to those who are new, lack the time, or do not have the technical expertise.

While recommendations and endorsements occur frequently in everyday conversations, they are often limited to private interactions such as text messages, group chats, and face-to-face discussions. These valuable exchanges of information are not captured at critical points where they would be most impactful, such as on Amazon at the point of purchase, on Spotify when discovering new music, or in MetaMask when signing an Ethereum transaction. This disconnect prevents the aggregation and public sharing of insights that could benefit a broader audience, thereby limiting the effectiveness of these platforms in providing comprehensive and trustworthy information.

4.2.2 Lack of Availability

For data to be truly useful, it must be not only captured but also made readily accessible. Presently, data is dispersed across various mediums, each with varying degrees of openness. The original vision for the internet, as envisaged by pioneers like Tim Berners-Lee, was to create an open and interoperable platform, epitomized by concepts like the Semantic Web. This vision aimed to facilitate seamless data exchange and integration across the web; however, reality has diverged significantly from this ideal.

In the current landscape, many Web2 companies have erected barriers around their data, often restricting access through paid APIs to protect their competitive advantages. These data silos have become critical assets for these companies, transforming data into a highly guarded commodity. This approach undermines the foundational principles of openness and interoperability that the internet was meant to uphold.

In contrast, the Web3 ecosystem, driven by a different ethos, generally promotes open access to data. Despite this, data fragmentation remains a significant issue, impairing its usability. For instance, decentralized social media platforms, though aligned with the principles of Web3, often lack interoperability with one another due to competing standards. This fragmentation complicates the integration and comprehensive use of data, making it challenging to achieve the seamless interaction envisioned for the decentralized web.

4.2.3 Standards and Data Fragmentation

Assuming that data is available, data usability also necessitates addressing the pervasive issue of data fragmentation, particularly within the permissionless Web3 ecosystem. Data fragmentation arises predominantly from challenges related to data structuring and standard/schema fragmentation.

Common standards, like the ERC-20 protocol for tokens, form the backbone of the permissionless Web3 environment. Without these standards, organizing in a distributed way would be exceedingly difficult. Different systems cannot effectively communicate or share data, isolating information within each silo.

The lack of standardized data formats and the proliferation of disparate schemas present substantial obstacles. This absence of uniformity hinders data composability, obstructs the seamless integration of services, and degrades the user experience. In Web3, these issues are a continuation of those seen in Web2, where rampant

Archived copy · cryp2nova.com

fragmentation renders verifiable data sets largely irreconcilable for advanced use cases, particularly those involving reputation systems.

For example, most attestation and verifiable platforms maintain their own distinct schema registries, which leads to further fragmentation. Even within a single platform like the Ethereum Attestation Service (EAS), schemas can vary significantly across different chains. This diversity in schema representation for similar data types complicates reconciliation, particularly when attempting to align fields across different schemas. This complexity makes it challenging to develop effective query and aggregation tools on top of the verifiable data set.

To address these issues, initiatives are developing common protocols and frameworks. The Decentralized Identity Foundation (DIF) and W3C work on interoperable standards for digital identities and credentials to ensure effective communication and data sharing across platforms. Protocols like IPFS and Ceramic Network enhance interoperability and data composability by facilitating cooperative decentralized data creation, storage, and sharing. Initiatives like schema.org contribute to standardizing data schemas, promoting consistent data representation across platforms.

However, developing and agreeing upon universal standards is often slow and contentious, referred to as "standards hell." Platforms frequently develop and defend their own protocols, leading to further fragmentation. This lack of common standards complicates interoperability, making it challenging for users to transition between services and for applications to leverage identity data across ecosystems.

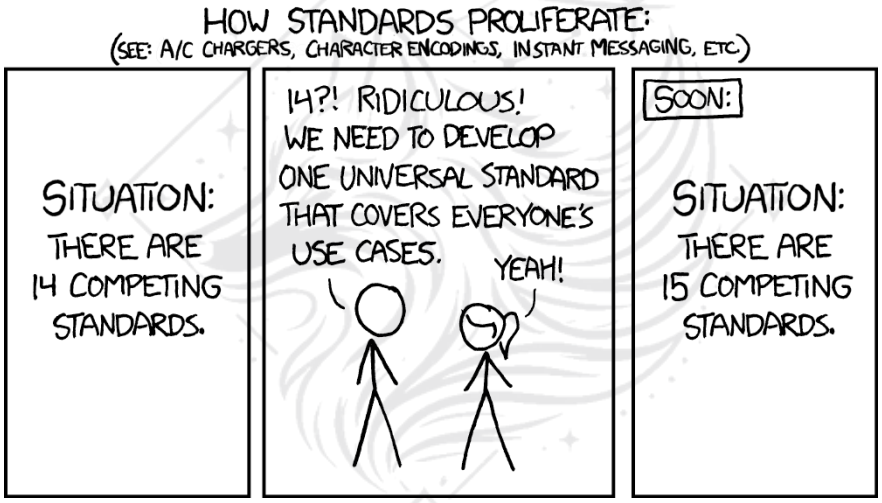


Figure 8: https://xkcd.com/927/

4.2.4 Lack of Discoverability

Even when valuable data is generated, made available, and potentially standardized, it frequently remains inaccessible due to poor discoverability. The absence of robust search and indexing mechanisms complicates data discovery, making it challenging for users to locate relevant information. Crucial data, such as security audit reports, user sentiment, and other critical insights, are dispersed across various platforms like GitHub, Twitter, Farcaster, and project-specific forums. This dispersion undermines the transparency and accountability of decentralized systems, as users struggle to access comprehensive and reliable data.

Consider, for example, a scenario where information about a specific product is scattered across multiple platforms. Even if the data about the product is accessible and standardized, the lack of a canonical identifier for the product makes it difficult to know where to search for this data. Users might find reviews on Amazon, technical specifications on the manufacturer's website, user discussions on Reddit, and visual content on Instagram. Without a unified identifier linking all this information, discovering and aggregating the relevant data becomes an onerous task.

While many aggregators exist in both Web2 and Web3, they introduce a new layer of complexity to the trust stack. Reliance on centralized aggregators can create dependency issues. If these platforms experience outages, technical failures, or malicious attacks, or if they become biased, manipulated, or decide to present only one side of the data, the accessibility of critical information is compromised. This dependency

Archived copy · cryp2nova.com

fundamentally undermines the decentralized ethos of blockchain technology, which prioritizes resilience and distributed control. Hence, while aggregation and indexing are essential for enhancing data discoverability, they must be implemented in ways that preserve the decentralized nature of the systems they support.

4.2.5 Lack of Comprehensibility

Data is only valuable if it can be properly interpreted. While data availability, standardization, interoperability, and discoverability are essential for accessing data, they do not inherently make data useful. The true value of data lies in its comprehensibility—users' ability to understand and derive meaningful insights from it.

For instance, consider on-chain transactions. While these transactions contain implicit signals, the true meaning behind them is not always clear. Take the example of a user depositing money into a DeFi protocol. This action may or may not indicate trust in the protocol, belief in its long-term viability, or simply an attempt to achieve high yield in the short term. Understanding the true intent is impossible, and inferring even some relevant signal often requires sophisticated analysis tools and contextual knowledge, which many users lack.

Data must also be presented within a semantic context to be comprehensible. Raw data without context is often meaningless. Structuring data using well-defined schemas and ontologies helps convey relationships and significance. For example, in a dataset of product reviews, it's crucial to understand the relationship between the reviewer, the product, and the review content to extract meaningful insights.

Relevance is another critical factor. In the decentralized web, users often encounter an overwhelming amount of information. Filtering and prioritizing data based on the user's specific needs and context enhance comprehensibility. For example, a user seeking trustworthy product reviews should be able to filter reviews by criteria such as the reviewer's reputation, the review date, and relevance to their query.

Furthermore, user experience plays a crucial role in data comprehensibility. This involves designing user interfaces that make data easily accessible and interpretable. Effective data visualization, straightforward navigation, and contextual information can significantly enhance the user's ability to understand and utilize the data. The focus should be on creating a seamless and intuitive experience that reduces cognitive load and helps users make sense of complex information.

5 Data Quality and Bias

5.0.1 Subjective Data Capture & Structuring

Current decentralized identity, verifiable claim, and attestation systems predominantly focus on deterministic truths and verifiable information, often neglecting the importance of subjective data. This emphasis on verifiable data means that subjective experiences, opinions, and nuanced information are frequently overlooked or undervalued. A comprehensive trust framework must accommodate subjective data, recognizing that not all valuable information can be objectively verified.

These systems typically prioritize cryptographically verifiable data, such as identity credentials issued by trust anchors and transactional records. While this approach significantly enhances security and reliability, it fails to capture the richness of subjective data essential for a more holistic understanding of trust and reputation. Subjective data, including personal experiences, opinions, and qualitative assessments, offers critical insights that deterministic data alone cannot provide.

Adapting these systems to accommodate subjective data requires significant changes in data handling and processing methodologies. This includes developing advanced algorithms that can interpret and integrate qualitative data into existing data structures without compromising the integrity and reliability of the system.

Moreover, there is a cultural aspect to consider. In many decentralized communities, there is a strong emphasis on verifiability and objectivity, often at the expense of subjective insights. Changing this culture to value and prioritize subjective data as equally important requires concerted efforts in education and community engagement.

5.0.2 Platform-Induced Expression Bias

Platforms often create environments that subtly coerce users into expressing specific things, driven by the design of the platform itself. Many platforms employ gamification techniques to encourage behaviors such

Archived copy · cryp2nova.com

as liking, sharing, or commenting. While these techniques can increase engagement, they often result in superficial interactions that fail to capture the full depth of user expression. The platforms' algorithms and interface designs are tailored to maximize user interaction and retention, but this frequently comes at the expense of genuine, nuanced expression.

The reputation data and signals that arise from these interactions are thus filtered through the platform's design biases. For instance, users may be incentivized to present an overly positive or curated version of themselves to gain more likes or followers, leading to a representation that is not necessarily reflective of their true selves. Similarly, the pressure to conform to popular opinions or trending topics can stifle authentic discourse and reduce the diversity of viewpoints shared on the platform.

This dynamic is particularly evident in social media environments, where the pursuit of virality and engagement can overshadow meaningful communication. Users might prioritize content that is more likely to be liked or shared, rather than content that genuinely reflects their thoughts or values. As a result, the reputation signals generated on these platforms can be misleading, as they are heavily influenced by the platform's incentives rather than the users' authentic expressions.

5.0.3 Imposition of Rigid Models of Truth

Many existing systems attempt to impose a singular model of truth through scores and verification mechanisms, which can be overly opinionated and inflexible. These systems often present information as definitive and unchallengeable, failing to accommodate diverse perspectives and the complexity of subjective reality. This approach can alienate users who do not align with the imposed standards and make it difficult to achieve consensus within the community.

Even platforms that strive for objectivity, such as Wikipedia, are fundamentally constrained by their editorial policies and community norms. While Wikipedia aims to present a neutral point of view, it often ends up enforcing a rigid model of truth that does not offer a platform for diverse perspectives. The content on Wikipedia is subject to the biases of its contributors and editors, and consensus on contentious topics can reflect the prevailing views of a limited subset of users rather than a balanced representation of all perspectives.

This imposition of a rigid model of truth can stifle innovation and discourage meaningful discourse. In a decentralized and diverse digital landscape, it is crucial to create systems that can accommodate multiple viewpoints and recognize the validity of subjective experiences. Systems that enforce a single version of the truth fail to capture the richness of human knowledge and understanding, limiting their utility and relevance.

This issue is compounded by the lack of robust reputation or reputation discovery mechanisms and the absence of verifiable attribution for most data. Without these tools, it becomes challenging to discern when information is biased or manipulated.

5.0.4 Complexity of User Interfaces

Many decentralized applications (dApps) currently suffer from user interfaces (UIs) that are not intuitive or user-friendly, particularly for non-technical users. The complexity of these interfaces can be a significant barrier to entry, limiting broader adoption and preventing mainstream users from engaging with decentralized technologies.

One of the primary challenges is the prevalence of technical jargon and concepts that are unfamiliar to the average user. Terms like "private keys," "gas fees," "smart contracts," and "staking" are commonplace in dApps but can be confusing and intimidating for those not well-versed in blockchain technology. This steep learning curve can discourage potential users from exploring and utilizing decentralized applications.

Another issue is that the processes involved in executing transactions on blockchain platforms often require multiple steps, each with its own set of instructions and considerations. For example, to interact with a decentralized finance (DeFi) platform, a user might need to connect a wallet, approve transactions, manage gas fees, and ensure the security of their private keys. Each of these steps involves specific knowledge and careful attention, increasing the likelihood of user error and making the experience cumbersome.

The complexity of dApp interfaces can also exacerbate security concerns. Users who do not fully understand the processes or technologies they are interacting with are more susceptible to phishing attacks, scams, and other malicious activities. Simplifying the UI and providing clear, easy-to-understand security warnings can help mitigate these risks, but this requires a concerted effort in design and user education.

Archived copy · cryp2nova.com

While wallet providers like MetaMask and Coinbase Wallet continue to enhance their interfaces to make them more user-friendly and secure, the persistence of hacks and scams demonstrates the ongoing immaturity of the crypto user experience. Despite advancements, the frequency with which users lose funds due to phishing, poor key management, and complex transaction processes highlights the critical need for improved UI/UX design and user education.

5.1 Authenticity, Security, and Privacy Challenges

5.1.1 Sybil Attacks

Sybil attacks are a significant threat to any decentralized system, particularly those where creating new identifiers involves minimal friction or cost. In a Sybil attack, an individual or entity creates multiple fake identities to manipulate or disrupt the network. These attacks can distort reputation systems, voting mechanisms, and other trust-based interactions, thereby undermining the reliability and fairness of the system. Preventing Sybil attacks requires robust mechanisms to ensure each identity within a network is unique and verifiable.

To counter Sybil attacks, various mechanisms can be employed:

- **Proof of Work (PoW)** and **Proof of Stake (PoS)** mechanisms increase the cost of creating multiple identities, making it economically unfeasible for attackers.
- **Proof of Humanity** verifies the uniqueness of individuals through social verification, biometrics, or attestations, ensuring that each identity represents a real person.
- **Web of Trust** builds a network of trust through endorsements from verified users, leveraging social structures to validate identities.
- **Zero-Knowledge Proofs (ZKPs)** allow for privacy-preserving verification of identity attributes, ensuring uniqueness without revealing sensitive information.
- **Identity Verification Services** can provide additional security layers by verifying identities through official documents and biometric data, though this may introduce centralization risks.

However, each of these solutions comes with trade-offs, and no perfect solution has yet been found.

5.1.2 Verifiable Bridging of Off-Chain Data to On-Chain Systems

Decentralized systems often need to interact with data that originates off-chain. Bridging this data to trustless systems in a verifiable manner is crucial for maintaining trust and integrity. The main challenges include ensuring data integrity, confidentiality, and availability during the transfer process.

Numerous teams are actively working on addressing these issues, employing advanced techniques such as decentralized oracles and zero-knowledge proofs to enhance the reliability and security of data transfers- however, despite these efforts, solving the problem entirely remains a monumental task, demanding continuous innovation and collaboration across the entire ecosystem.

5.1.3 Data Provenance

Data provenance, the ability to trace and verify the origins and history of data, is a significant challenge across the web. Despite the existence of tools designed to address this issue, they have not fully delivered on their promises.

In the traditional web, data is often siloed within proprietary platforms, making it difficult to track its journey from creation to consumption. This fragmentation undermines the reliability and trustworthiness of information, as users have no way to verify the authenticity and integrity of the data they encounter. Misinformation and data manipulation become prevalent, eroding user trust.

Various tools and frameworks have been developed to tackle data provenance. Blockchains, decentralized data storage solutions, and other cryptographic toolings offer mechanisms to record and verify the history of data transactions in a tamper-proof manner. These solutions aim to provide transparency and accountability, ensuring that data can be traced back to its original source.

However, the practical implementation and widespread adoption of these tools have been lacking. In an era where AI-generated content is frequently mistaken for human-created data, and deep fakes are increasingly

Archived copy · cryp2nova.com

common, the failure to fully implement robust data provenance mechanisms leaves us vulnerable to rampant misinformation and deception.

5.1.4 Balancing Transparency and Privacy

The concept of "data as a public good" is highly beneficial for enhancing our ability to make informed decisions, fostering transparency, and ultimately aiding in building a trustful interaction layer. The more accessible and transparent data we have, the better our perspectives and decisions can be. However, privacy remains a crucial concern. As we strive for greater transparency, it is equally important to ensure that individuals' privacy is protected. Building systems that accommodate both public and private data is essential for creating a balanced and trustworthy digital ecosystem.

Balancing transparency and privacy involves implementing selective disclosure mechanisms and privacy-preserving technologies. Solutions such as homomorphic encryption and Zero-Knowledge Proofs (ZKPs) enable users to reveal specific data attributes without exposing the entire dataset, bolstering the potential of selective disclosure systems. Homomorphic encryption allows data to be processed while still encrypted, ensuring confidentiality throughout the process. ZKPs allow users to prove the validity of a statement without revealing the underlying data, maintaining privacy while ensuring authenticity.

However, despite these advancements, balancing transparency and privacy in decentralized systems remains an unsolved problem. One of the primary challenges is the inherent tension between the two goals. Transparency requires data to be openly accessible and verifiable, while privacy necessitates keeping certain information confidential. This tension is particularly pronounced in decentralized systems where the principle of transparency is foundational.

6 The Current State of Affairs

> "Show me the incentive and I will show you the outcome" - Charlie Munger

Despite significant technological advancements that hold the promise of creating a trustful interaction layer, this issue remains largely unresolved. Effective and efficient decision-making depends on the availability of high-quality data. Although infrastructural tools such as platforms for creating verifiable claims exist and can aid in this process, they have yet to reach their full potential. This is evidenced by the frequent lack of access to critical data at crucial moments. Consequently, users often make poor decisions, leading to a suboptimal Web3 experience. Many individuals find themselves in inappropriate communities, investing in unsuitable projects, or interacting with malicious contracts. This misalignment significantly hampers the potential benefits of decentralized systems, often making trustlessness more of a liability than an asset.

Given these challenges and the fact that ***some*** users can navigate Web3 successfully (indicating that the necessary data exists ***somewhere***), there is an urgent need for a system that leverages collective intelligence to enhance decision-making. Such a system would introduce greater trust in environments or situations where complete cryptographic verification and trustlessness are not yet possible.

In the examination of the host of aforementioned problems currently blocking the realization of a trustful interaction layer, each can be largely attributed to a breakdown in social participation, coordination, and consensus. For example, the lack of consensus on identity standards leads to fragmented digital identities across platforms, making it difficult to establish cohesive online personas. Similarly, the absence of unified data standards and schemas results in incompatible data formats, hindering interoperability and data integration. Moreover, the scarcity of data itself hampers the ability to derive meaningful interpretations.

Fortunately, the blockchain sector stands at the forefront of coordination technology, providing crucial insights for overcoming these challenges. Intuition harnesses the economic principles that currently secure and sustain Web3, applying them to incentivize participation and foster consensus on identifiers and information. This strategy seeks to establish a credibly neutral framework that leverages collective intelligence to inform and guide user interactions. By tapping into the wisdom of crowds, Intuition extends the capabilities of coordination technologies, creating a system that bolsters trust in areas that cannot yet be made fully trustless.

Archived copy · cryp2nova.com

7 Core Guiding Principles of Intuition

Through the examination of the current state and the persistent challenges of deriving trust in all our interactions, it becomes clear that the problem should be addressed through a composition of various decentralized identity, data, and finance primitives. Leveraging these tools, we can build robust systems that encourage better expression, curation, standardization, interpretation, and discoverability of data. By adhering to the following principles, we can create a framework that promotes fairness, inclusivity, and interoperability:

Credibly Neutral

The protocol should be credibly neutral, just as all protocols managing identities, data, and algorithms should. A credibly neutral system should operate impartially, without favoring any particular group, perspective, or outcome. This neutrality is essential for fostering trust and inclusivity within the ecosystem, ensuring equitable treatment for all participants.

Unopinionated Protocol

The protocol should remain unopinionated, imposing no restrictions or biases on the types of claims that can be made - just as the internet does not impose restrictions on the transfer of arbitrary data. This stance allows users to claim anything about anything, supporting diverse voices and perspectives. Higher-level middleware and applications can implement filters and moderation mechanisms to prevent abuse while preserving the core protocol's neutrality and openness.

No 'Truth Lock In'

The system should accommodate all viewpoints on any issue, rather than presenting only the prevailing opinion. This requires an absence of vendor lock-in. Users should be able to toggle between different perspectives, ensuring a spectrum of views. This flexibility prevents the platform from becoming a gatekeeper of information, maintaining the decentralization ethos. Moreover, developers should be able to create new methods for filtering and presenting data without requiring permission. This permissionless innovation ensures that diverse methodologies for data distillation can flourish, catering to the varied needs and preferences of the user base.

Self-Sovereign Identity

Users should be able to control their digital identities, managing, sharing, and protecting their information without relying on centralized authorities. This enhances privacy and security, fostering a user-centric digital ecosystem. Enabling self-sovereign identity promotes user autonomy and trust, allowing individuals to interact confidently and securely across various platforms and services.

Self-Sovereign Data

Users should have sovereignty over their data. Decentralizing control mitigates risks such as censorship and data breaches, ensuring users retain full ownership and control over their data and enabling novel monetization opportunities.

Public and Private Data Options

Users should be able to choose whether their data is public or private, controlling its visibility and privacy, especially to select entities or groups. Offering encryption and permission settings facilitates a secure and customizable data environment, prioritizing user autonomy and security, and creating data flow rails where data can easily make its way to the places it needs to be and to the people and machines who need it, securely.

Verifiability

Where applicable, all data should be signed with self-sovereign private keys and referenced with Decentralized Identifiers. This facilitates data provenance and authenticity, extending verifiability across all layers of the stack, including data, queries, reputation, scores, and algorithms - which should also be made verifiable, ensuring that the data presented to users and developers remains tamper-resistent throughout its lifecycle.

Data Integrity and Security

Robust cryptographic techniques and decentralized storage solutions should be employed to ensure data remains tamper-proof, available, and secure.

DIDs, For Everything

Archived copy · cryp2nova.com

Every entity and concept should have a globally persistent decentralized digital identifier. Assigning Decentralized Identifiers (DIDs) to all entities ensures decentralized control and referenceability across the web, achieving true decentralization and interoperability.

Decoupling of Identities, Data, and Algorithms from Applications

The system should establish a foundational layer that effectively decouples identities, data, algorithms, and their interrelationships from specific applications. This decoupling is essential for achieving the flexibility, interoperability, and neutrality required for a robust and inclusive digital ecosystem. Through this separation, the system should allow all applications across the web to tap into a unified, semantic, distributed, and verifiable data lake which hosts identities, data, and algorithms.

Composable Data

Data should be maximally utilizable, meaning it must be structured in a way that allows for easy integration and interoperability across various systems and applications. By ensuring data is composable, we enable it to be combined, reused, and extended in multiple contexts, fostering innovation and efficiency. This approach not only enhances the value and utility of data but also facilitates a seamless user experience, where information flows freely and meaningfully across different platforms.

Semantic Data

The data within Intuition should be semantic, enabling the addressing of complex use cases, particularly around reputation. By ensuring that data is structured semantically, Intuition allows for nuanced and sophisticated queries and analysis, making the data more actionable and valuable. This approach enhances the ability to capture and leverage complex relationships and attributes, providing deeper insights and supporting advanced applications.

Convergence on Canonical Identifiers through Incentives

Economic and social incentives should drive consensus on canonical identifiers for all entities, rather than centralized imposition. This organic convergence on canonical identifiers for all things allows those things to be uniformly referenced across the web without reliance on centralized intermediaries, fostering a more cohesive digital environment.

Permissionless Folksonomy The system should enable organic convergence on descriptors and classifications without formal standards committees. Leveraging social consensus allows the community to evolve and adopt common models dynamically, promoting flexibility and inclusivity.

Convergence on Standards through Incentives

Standards convergence should be achieved through economic incentives and natural user behavior rather than committee debates. Incentivizing users to adopt common standards and data structures minimizes fragmentation and aligns the system with practical and widely accepted conventions.

Blockchains for Financial Transactions and Time-Series Data Blockchains or analogous systems should store time-series data and manage financial transactions, ensuring historical data accuracy and tamper-proof verification. This approach also supports the construction of permissionless value flow rails for data, an essential component of data monetization democratization.

Portability of Identity, Data, and Reputation

Intuition should support the portability of identity, data, reputation, community, and preferences, enabling continuity and control across different platforms and applications, and aiding in the prevention of vendor lock-in.

Generalized Use Case Accommodation

The system should support a wide range of applications and scenarios, ensuring broad applicability and avoiding fragmentation. This generalizability is essential for maximizing convergence on a singular system, which is optimal for the effectiveness and utility of the system. Just as the internet's generalizability and openness have enabled it to support countless applications and use cases, the system should be sufficiently generalized to serve as a foundational layer for various decentralized applications and interactions.

Incentivized Participation

Archived copy · cryp2nova.com

Participants should receive value for the creation and sharing of valuable data, as the time, energy, and attention put into creating and sharing valuable data is inherently valuable. Programmatic value flows should reward users for meaningful contributions, driving active participation and high-quality data creation.

Openness and Interoperability

The protocol should be open and interoperable, facilitating seamless integration with other systems. This openness enhances the utility and reach of the data and services provided.

Intuitive User Experience

The user experience should be prioritized, ensuring accessibility and ease of use. Intuitive interfaces and interactions lower the barrier to entry and encourage broader adoption. Many of the other tenants can only hold true in the presence of good UX - for instance, data is not truly self-sovereign if a user does not know how to access, manage, and utilize it.

Decentralized Control and Ownership

Anyone should be able to store and replicate the state of the system from scratch without permission. This openness fosters transparency, trust, and innovation, maintaining the integrity of the decentralized system. While specialized tools and interfaces may be developed to facilitate interaction with and interpretation of the data, the raw data itself should remain freely available and accessible.

Decentralized Governance

The protocol should be governed by its user community. Implementing decentralized governance mechanisms ensures all stakeholders have a voice, promoting transparency and inclusivity. This democratic approach fosters a sense of ownership and accountability within the community, aligning the protocol's development with the collective interests and values of its users.

Aligning Interests of Users and System

The system should align the best interests of the users with the best interests of the system. Examples such as Bitcoin and Ethereum demonstrate how aligning incentives can lead to robust and sustainable ecosystems. The system should create a similar alignment, ensuring that the success of the system and the satisfaction of its users are inherently interconnected.

By adhering to these core guiding principles, Intuition aims to create a robust, decentralized trust framework that empowers users, fosters collaboration, and enhances the overall reliability and functionality of the web3 ecosystem. These principles serve as the foundation for all of Intuition's development efforts, ensuring that the protocol remains true to its mission and values.

CRYP2NOVA

8 The Intuition System

8.1 Introduction

Guided by the aforementioned principles, Intuition is designed as a transformative solution to address the layers of the decentralized web that cannot yet be made entirely trustless. By capturing, structuring, and serving useful data, Intuition aims to create trust**ful** environments where reliable information empowers users to make more informed decisions. Leveraging the principles of decentralization, Intuition harnesses collective intelligence to enhance the trustworthiness of all digital interactions.

8.2 What is Intuition?

Intuition is a cryptoeconomic protocol that makes verifiable data easy to create, manage, and use. With this, it aims to transform how digital trust is established and maintained by integrating incentive-driven contribution mechanisms, decentralized identifiers, and semantic data structures, to create a decentralized semantic web of trust.

Intuition fulfills this promise through several key innovations:

Incentive-driven social consensus on globally persistent canonical identifiers

Archived copy · cryp2nova.com

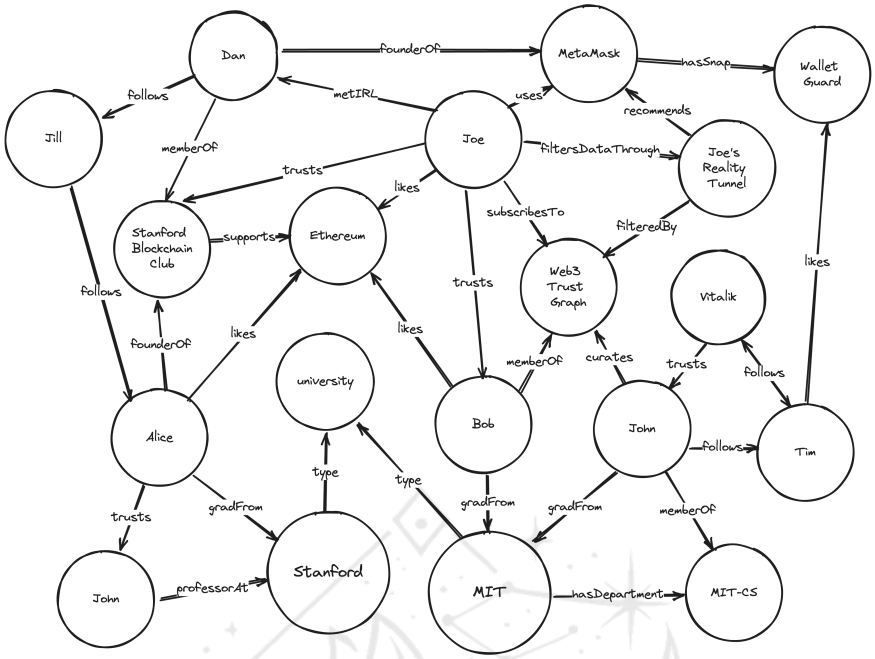


Figure 9: 2-dimensional reductionist representation of the Intuition Trust Graph

Intuition employs a system of economic incentives to drive social consensus around universally recognized and interoperable identifiers for all entities, concepts, and data. These identifiers serve as the digital anchors for entities, concepts, and data across the web, ensuring consistent and reliable references. This approach is designed to mitigate data fragmentation and promote uniformity in how things are represented across the digital ecosystem.

Incentive-driven, many-to-one, deterministic and non-deterministic attestations

Intuition introduces a novel approach that facilitates and encourages the creation of both objective (deterministic) and subjective (non-deterministic) 'attestations' in a many-to-one manner. This method helps to generate a comprehensive and reconcilable dataset, incentivizing users to contribute valuable data regularly through economic rewards.

Incentive-driven structuring and standardization of attestation-based expression

Intuition incentivizes the convergence on standardized formats, structures, and schemas for verifiable data, thereby making data more semantic, interoperable, and consumable. By encouraging social consensus around uniform formats, structures, and schemas, Intuition ensures that data can be easily understood, processed, and integrated across various platforms and applications, without the need for the top-down imposition of rigid standards. This structured approach not only enhances the semantic richness of the data but also facilitates more complex and meaningful interactions that would be challenging to achieve in a fragmented data environment, making attestations a viable meta for human expression.

A permissionless platform for interpretation of the wisdom of the crowds

Intuition offers a decentralized framework where different interpretations of data can coexist, enabling a rich and diverse ecosystem of applications and services. In stark contrast to platforms which attempt to adjudicate the truthfulness, correctness, or validity of data, Intuition's mechanics are designed to function in the absence of the imposition of rigid models of 'truth'. This openness allows developers and users to bring their own unique perspectives, insights, and innovations to Intuition, enhancing the platform's overall versatility and utility. By encouraging and facilitating the permissionless interpretation of data, Intuition encourages a continual examination of interpretation techniques, immunizing the system against bias or manipulation.

Archived copy · cryp2nova.com

8.3 Overview of the Primitives

8.3.1 Atoms

A system facilitating the arrival at social consensus around globally persistent canonical identifiers for all things demands that these identifiers possess a few key attributes.

Firstly, these identifiers should be decentralized identifiers, providing unique, secure, and verifiable identification without any reliance on a central authority.

Secondly, these identifiers should have a sufficient amount of associated data to ensure precise referencing of specific entities, concepts, or pieces of information. Without this contextual data, it would be unclear what each identifier is meant to represent.

Thirdly, these identifiers must have some agent-centric state that is capable of tracking the usage of the identifier across contexts. This enables the community to discern which identifiers are being most frequently used to represent different concepts in different settings.

To solve for these requirements, the concepts of Atoms emerge as the foundation of the Intuition framework, representing the most fundamental units of data. These units can range from a single word to a complex concept, serving as discrete, manageable, and referenceable pieces of information that facilitate seamless data integration and manipulation across the web. By taking arbitrary data of any size and prescribing it a decentralized identifier, we can:

1. Start to reference data universally across the web.
2. Grant users equity in data as they signal its relevancy through usage.
3. Reward users for signaling the relevancy of data, thereby encouraging active participation and accurate data representation.

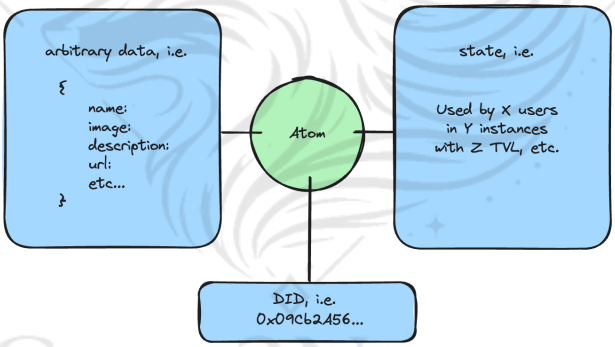


Figure 10: Basic overview of the key elements of an Atom

Each Atom is made universally referenceable through a decentralized identifier. This approach ensures that every Atom is uniquely identifiable and can be consistently referenced across the web, maintaining data integrity and meaning regardless of the system or context.

```
// An example DID

did:ethr:mainnet:0x3b0bc51ab9de1e5b7b6e34e5b960285805c41736

// An example DID Document

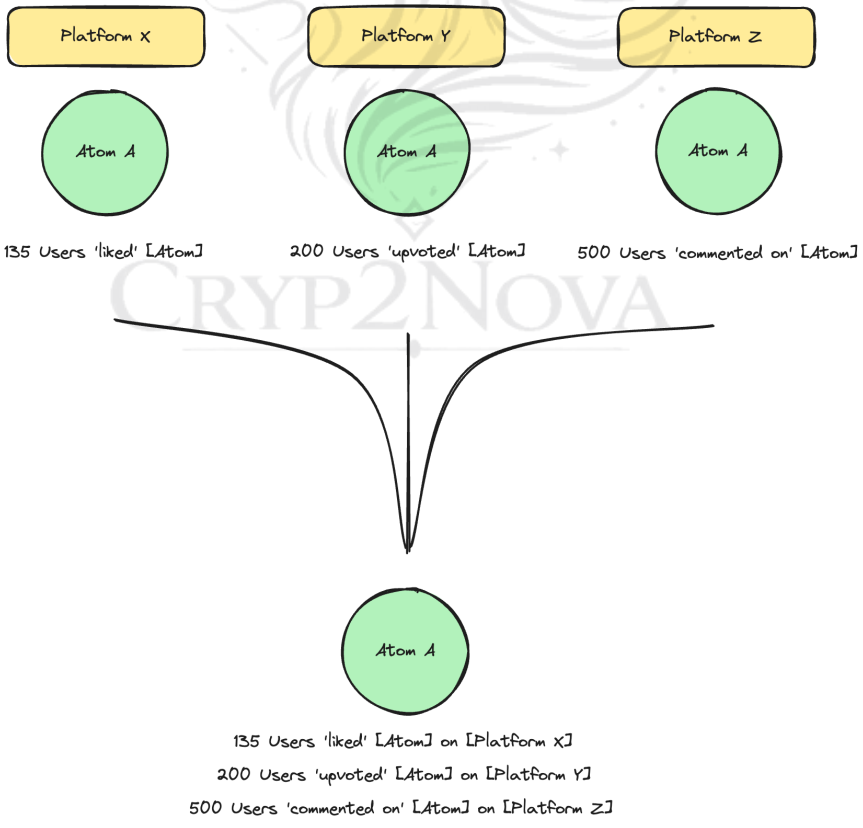
{
  "id": "did:ethr:mainnet:0x3b0bc51ab9de1e5b7b6e34e5b960285805c41736",
  "verificationMethod": [
    {
      "id": "did:ethr:mainnet:0x3b0bc51ab9de1e5b7b6e34e5b960285805c41736#controller",
      "type": "EcdsaSecp256k1RecoveryMethod2020",
      "controller": "did:ethr:mainnet:0x3b0bc51ab9de1e5b7b6e34e5b960285805c41736",
```


Archived copy · cryp2nova.com

```
      "blockchainAccountId": "eip155:1:0x3b0BC51Ab9De1e5B7B6E34E5b960285805C41736"
    }
  ],
  "authentication": [
    "did:ethr:mainnet:0x3b0bc51ab9de1e5b7b6e34e5b960285805c41736#controller"
  ],
  "assertionMethod": [
    "did:ethr:mainnet:0x3b0bc51ab9de1e5b7b6e34e5b960285805c41736#controller"
  ],
  "@context": [
    "https://www.w3.org/ns/did/v1",
    "https://w3id.org/security/suites/secp256k1recovery -2020/v2",
    "https://w3id.org/security/v3 -unstable"
  ]
}
```

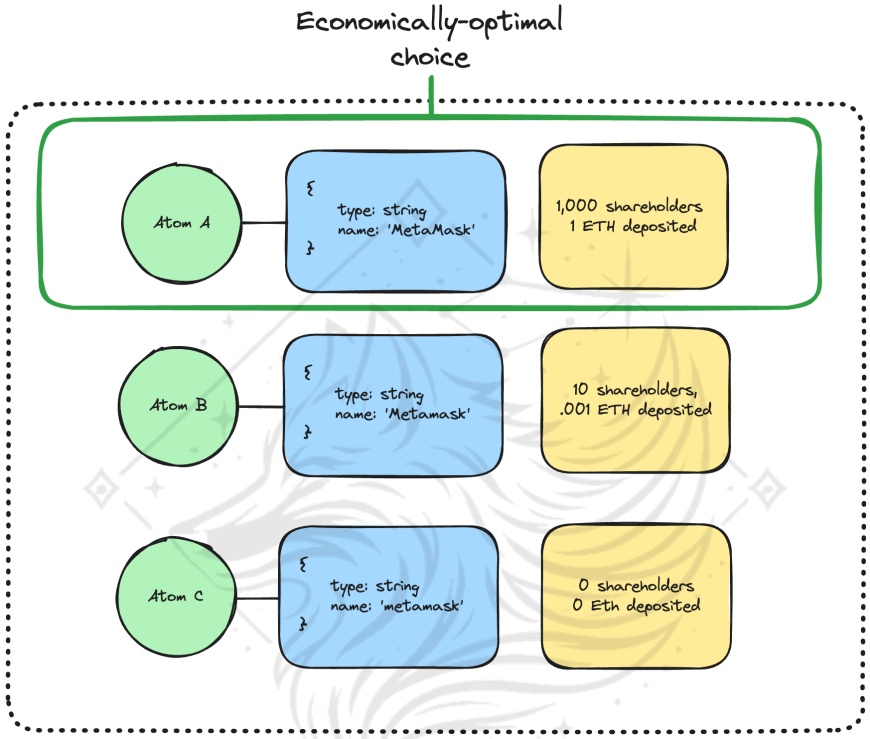
To provide guarantees around the entity/concept/data attempting to be referenced by the Atom, each Atom must have at least some de minimis corresponding data. This data can be anything, live anywhere, and take any format, though storing data in a Verifiable Data Registry and utilizing supported data structures and schemas is recommended, as it improves the usability of the data through strong guarantees around immutability, availability, liveness, and persistence. Atom uniqueness is enforced through a hash of this underlying Atom Data, ensuring that no piece of data can have two corresponding Atoms. To maintain the integrity of mutable data, it's crucial that any such data be timestamped. This ensures that any future references to the data clearly understand what the data was referencing at the specific point in time when the attestation was made.

Through this, Atoms enable the breakdown of data into discrete, manageable units, which can be easily combined and reused across various contexts and applications. This structuring supports flexible and adaptable digital systems, ensuring that data is interoperable across platforms. The composability of Atoms enhances the functionality and versatility of the system, allowing data to be efficiently utilized in different settings.



Archived copy · cryp2nova.com

Atom Ownership and Token Curated Registries Given the permissionless nature of the system, multiple Atoms may be representative of the same concept. To foster consensus on high-quality Atoms and establish canonical identifiers for all things, Intuition employs the concept of a Token Curated Registry (TCR). In this model, users gain fractional ownership over the Atoms they interact with and receive a portion of the interaction fees each respective Atom generates, incentivizing engagement with popular Atoms. As users increasingly interact with these Atoms, a TCR emerges, ranking Atoms based on their relevance using metrics such as an Atom's Total Value Locked (TVL). This mechanism facilitates ecosystem convergence on and easy discoverability of the most valuable and widely accepted Atoms/identifiers representing each concept.



8.3.2 Triples

With discrete units of data established through Atoms, defining relationships between these units to form higher-order structures is essential. Intuition achieves this by employing Semantic Triples, ensuring a uniform and discrete structure that can be prescribed a decentralized identifier and have some associated agent-centric state. This structure is essential for achieving consensus on arbitrarily sophisticated and expressive forms of data.

Triples consist of three elements: Subject, Predicate, and Object, with each element represented as an Atom. This Subject-Predicate-Object format allows users to clearly and explicitly define relationships between Atoms. These connections can be visualized as a graph where each node and edge is an Atom.

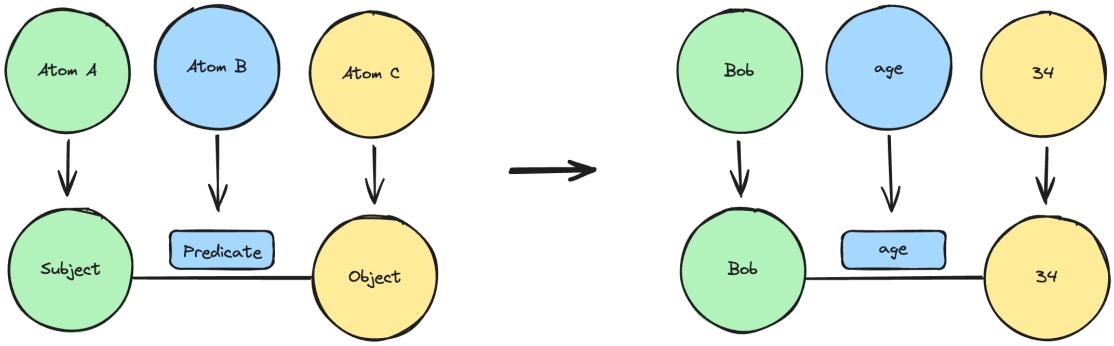
For example, a Triple may have the structure:

- **Subject:** "Bob"
- **Predicate:** "age"
- **Object:** "34"

In this example, each component—Subject, Predicate, and Object—is an Atom, and the Triple expresses a specific relationship between these Atoms.

Fractal Data Representations

Archived copy · cryp2nova.com



Triples offer a flexible yet structured method for representing data relationships. By allowing Triples to act as Atoms within other Triples, Intuition facilitates the expression, storage, and usage of arbitrarily complex data models that can scale and evolve over time. This flexibility is crucial for capturing intricate relationships and dynamics within data, enabling users to construct sophisticated applications and services on the Intuition framework. This approach maintains discrete, referenceable units for data at every layer of the structure, ensuring scalability and precision in data representation.

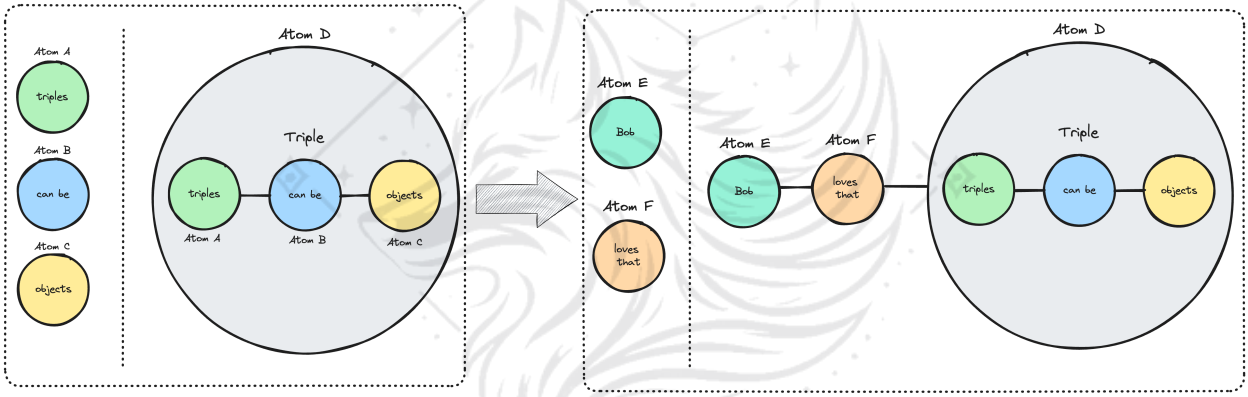


Figure 11: A Triple as an Object of another Triple

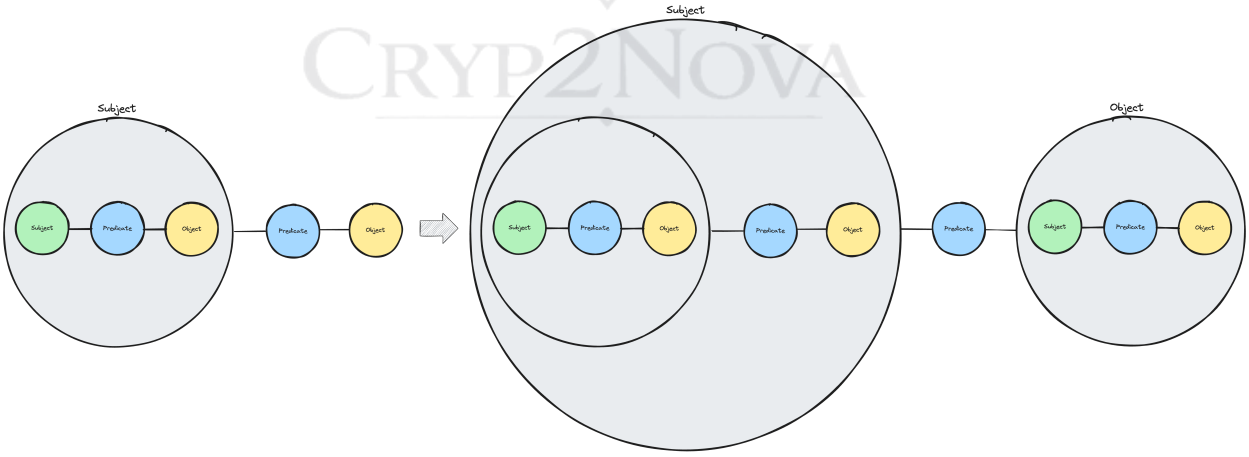


Figure 12: The flow of a more complex structure achieved through nested Triples

Triple Ownership and Token Curated Registries Akin to the process outlined for Atoms, the structure of Triples allows users to gain fractional ownership of Triples through interaction. Each interaction

Archived copy · cryp2nova.com

generates interaction fees, which are distributed to the owners of each respective Triple, creating an incentivized Token Curated Registry (TCR) for data structures. The TCR encourages system participants to adopt common ways of structuring data by offering economic rewards. This approach promotes an organic, incentive-driven structuring of data, contrasting with more rigid and traditional methods such as standards committees, which often struggle to achieve effective standardization.

8.3.3 Signal

Signal, in the context of Intuition, refers to any action or indication that expresses intent, belief, or support. Signals can be classified into two broad categories: explicit signals and implicit signals. These signals play a crucial role in interpreting user behavior, beliefs, and preferences within the system.

Explicit Signal

An explicit signal is a clear, intentional action taken by a user to express support, belief, or intent. These actions are directly observable and often involve a formal mechanism within the system. Examples of explicit signals include voting mechanisms, where casting a vote represents a user's preference. Verifiable claims and attestations are also forms of explicit signals; they are signed messages that convey specific information. For instance, a proof of humanity attestation from a trust anchor like Worldcoin is an explicit signal from Worldcoin that Worldcoin believes the entity to be human (a valuable data point for sybil resistance efforts).

Implicit Signal

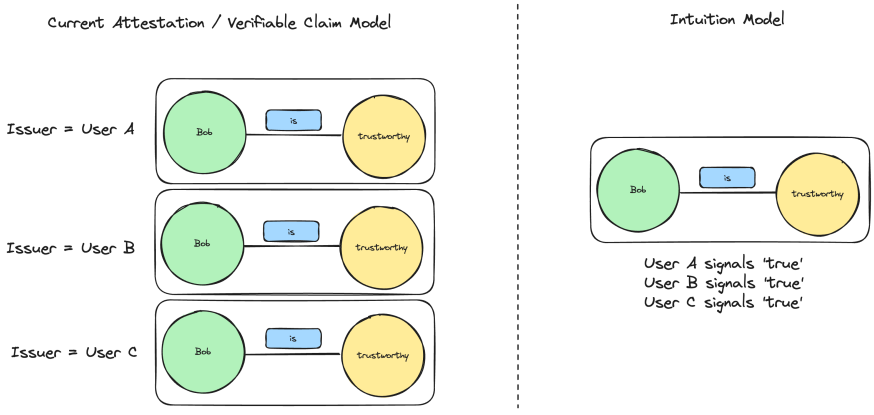
Implicit signal involves indirect or inferred indications of support, belief, or intent. This signal is not always directly observable and are often deduced from user behavior or patterns. For example, the frequency and context of user interactions with certain data points can imply their support or belief. Implicit signal requires sophisticated analysis to interpret accurately, as it is embedded within the user's activity data.

Transitive Signal

Transitive signal refers to the trust or belief that is passed along through a network of relationships. This type of signal leverages the idea that trust can be extended through connections. For example, if User A attests to something about User B, and User C trusts User A, then User C is likely to extend some level of trust to User B, even without a direct interaction. This transitive nature of trust is vital in decentralized systems like Intuition, where direct trust relationships are not always possible. By harnessing transitive signals, the system can create a more interconnected and trust-rich environment, where the credibility of one entity can influence the perception and trustworthiness of others within the network.

Signal in Intuition

Though all systems naturally generate implicit signal, explicit signal in Intuition is expressed in a novel format that enables and incentivizes the creation of many-to-one, non-deterministic attestations. In Intuition, these semantic statements do not have a single 'issuer' - instead, anyone/anything can signal support or rejection of any existing statement/attestation at any point in time. This decoupling of information from 'who is presently expressing/supporting that information' introduces the ability to accommodate many-to-one attestations, making the data significantly more usable - especially for more complex use cases that involve the concept of transitive signal, such as reputation.



Archived copy · cryp2nova.com

To accomplish this, the Intuition system enables users to maintain positions on Atoms and Triples, interpreting these positions as explicit signal from the user. This mechanism can be implemented using tokens or other accounting systems that have the ability to track user balances over time across an arbitrarily large number of entities.

Atom Signal

Within the Intuition framework, users signal their belief in the relevance of an Atom by adjusting their balance on that Atom. This balance can be increased or decreased arbitrarily.

A balance of zero implies no signal, while any positive balance indicates a degree of belief in the Atom's relevance. This mechanism is economically driven: users earn fees proportional to their ownership stake in an Atom as other users interact with it. Thus, if a user deems an Atom relevant, they are incentivized to signal its relevance to receive these rewards.

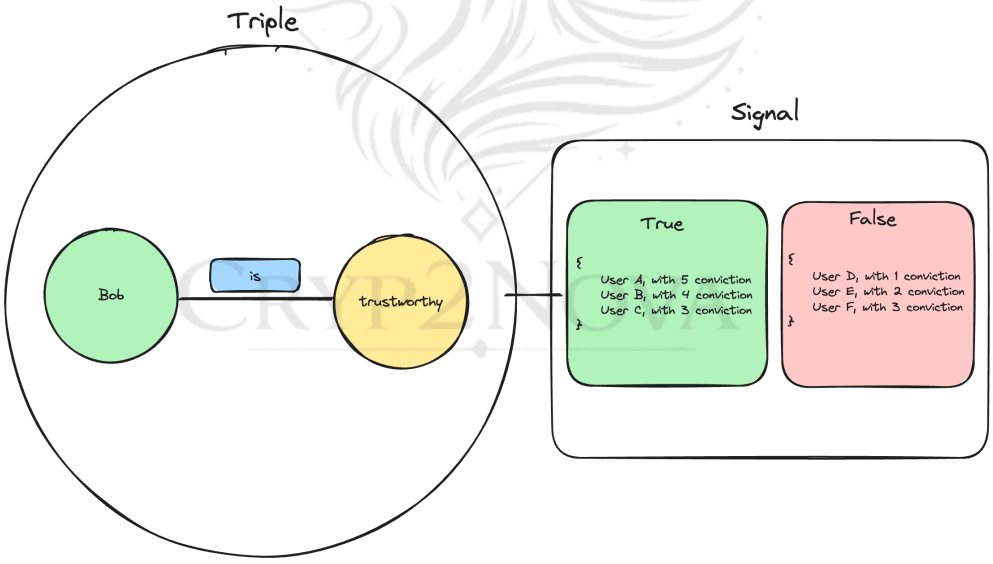
Negative integers may be used if the Intuition system's implementation aims to allow users to explicitly signal the irrelevance of an Atom. In systems without negative balances, the absence of a positive signal can serve as an indication of the Atom's irrelevance.

Triple Signal

In the Intuition framework, users signal their belief in both the relevance and truthfulness of a Triple by modifying their balance on that Triple. Triple balances can be any integer, allowing for a nuanced expression of belief.

A balance of zero indicates no signal. A negative balance signals a rejection of the Triple, explicitly indicating that the Triple is considered false, and that this falsehood is relevant. Conversely, a positive balance affirms the Triple, explicitly indicating that the Triple is considered true, and that this truthfulness is relevant.

For example, with a Triple asserting "[Vitalik] [is] [trustworthy]," users would express their belief in its truthfulness, and the relevancy of this truthfulness, by increasing their balance on the affirmative side of the Triple, or signal disbelief by decreasing their balance into the negative. This mechanism allows for nuanced expressions of trust and belief within the decentralized ecosystem.



This system enables each "statement" to exist in different states based on who is affirming or rejecting it. To illustrate the power of this approach, consider the example of building a decentralized list of followers. In a traditional one-to-one model, where each claim or attestation has a single issuer, if a user had 1,000 followers, there would be 1,000 separate "following" claims. Most of this data would be redundant, as the "following Y" part would remain constant across all claims. Additionally, this data would only be easily reconcilable assuming consistent standards and schemas across all claims.

In contrast, the Intuition model simplifies this by having a single Triple representing a statement such as "I am following Y." Users would then adjust their balances on this statement to express their stance. To see

Archived copy · cryp2nova.com

all followers of Y, one would simply examine the "I am following Y" Triple and identify who has positive balances on the affirmative side. This approach consolidates data, reducing redundancy and making it easier to verify and aggregate information.

Furthermore, the ability to adjust balances allows for a more nuanced expression of preferences. In the context of a 'follow' functionality, instead of a flat follow list where all followers are treated equally, users could explicitly signal varying levels of interest or endorsement. By increasing their balance on the followers they value more, users can effectively rank their follow list. This means that someone could show a stronger preference for certain individuals or entities by staking more tokens on their affirmations, creating a dynamic and tiered system of trust and preference. This not only enhances the granularity of data but also provides richer insights into user preferences and social dynamics within the network.

8.3.4 Fees & Economics

Interactions within the Intuition system incur a fee, comparable to a gas cost in blockchain transactions. This fee serves several essential purposes:

Firstly, in decentralized and permissionless systems with shared infrastructure, it is vital to prevent system abuse, such as Sybil and denial-of-service (DoS) attacks. Intuition mitigates these risks by employing an economic model similar to those in blockchain networks, necessitating a fee for data creation. This economic disincentive discourages abuse, thereby preserving the system's integrity and functionality. Furthermore, any attacks inadvertently benefit the network due to the fee payment, much like how Ethereum benefits from transaction fees even when used for non-productive purposes. This mechanism ensures the ecosystem remains robust and sustainable despite potential misuse.

Secondly, the creation of coherent and valuable data is often neglected, especially within the Web3 environment. Providing infrastructure for generating verifiable data alone has proven insufficient in motivating users to produce meaningful contributions. This issue is also prevalent in Web2, where the majority of users refrain from leaving reviews on platforms such as Amazon, Yelp, or Google, and rarely endorse others on LinkedIn or contribute to Wikipedia. Thus, there is a clear need for incentives to promote active and meaningful participation in the data contribution process, similar to how block rewards encourage participation in the layer 1 blockchain consensus process.

Thirdly, the sheer volume of data generated globally has reached overwhelming proportions, leading to an abundance of low-quality, redundant, or irrelevant information. This overabundance dilutes the value of truly meaningful and actionable data, complicating efforts to derive valuable insights. In both Web2 and Web3 environments, the emphasis needs to shift from merely producing more data to generating high-quality, reliable information. Intuition addresses this challenge by implementing mechanisms that discourage the production of irrelevant data and promote the creation of useful, pertinent information through economic incentives. By introducing an economic cost and associated rewards to data creation and curation, Intuition ensures that contributors are motivated to generate data that is coherent, valuable, and meets predefined standards of relevance and accuracy. This economic model not only deters the proliferation of "junk data" but also encourages the continuous refinement and validation of existing data.

Fourthly, the process of establishing standards in most industries has historically been fraught with difficulties, often described as "standards hell." This status quo has failed to adequately address the needs of our ecosystem. Intuition's system of trustless economic incentives expands the concept of leveraging financial rewards for distributed consensus—a principle successfully demonstrated in the blockchain ecosystem—to additional domains requiring social consensus and global coordination. These domains include standards for data structures, schemas, and formats, as well as canonical identifiers to which this data can be attached and correlated.

Intuition's imposed fees addresses these challenges in two main ways:

1. **Granting Ownership in Data**: A portion of the fee contributes to granting the user ownership in the data they interact with. This mechanism ensures that users have a vested interest in the data they create or engage with, promoting responsible and meaningful interactions.

2. **Rewarding Data Owners**: A portion of the fee is distributed to existing owners of the data being interacted with. This incentivizes the creation and maintenance of valuable data, as users receive economic rewards for their contributions to the ecosystem.

Archived copy · cryp2nova.com

This flow of value is enabled by Intuition's innovative approach to data representation, which encompasses Atoms, Triples, and Signal. By structuring data into fractals via discrete, ownable fragments, this model allows for the programmatic distribution of value throughout the system's state.

Consider a user who wishes to create a new data entry stating that they like a YouTube video. The user must pay a fee to create this data, part of which grants them ownership in the statement and part of which rewards previous owners of related data. Other users who agree with this statement can also pay a fee to do so explicitly, reinforcing the validity and increasing the value of the data. This process helps to ensure that only high-quality, relevant data remains prominent, as users are financially incentivized to support accurate and meaningful information.

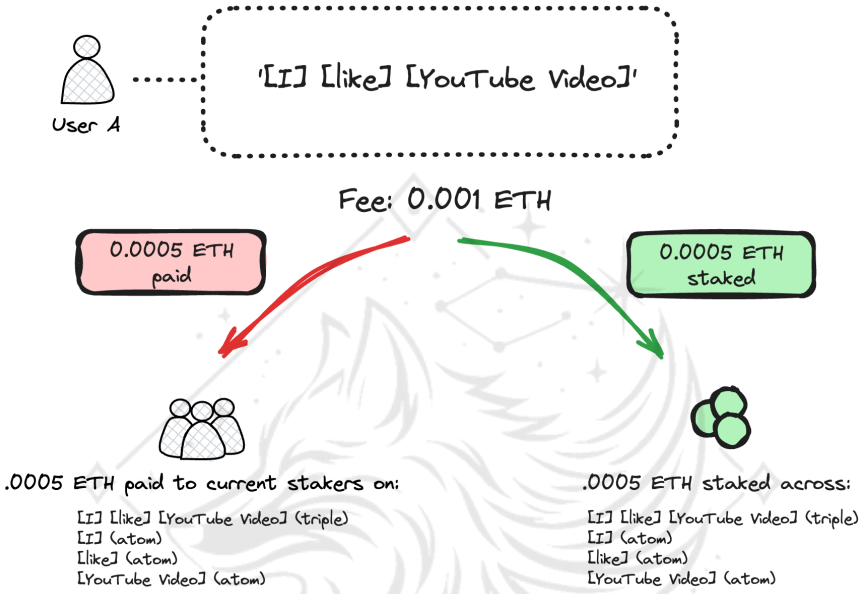


Figure 13: A demonstration of the high-level flow, with arbitrary example numbers.

This economic model encourages users to interact with data they believe will attract further engagement. Because data structures in Intuition are explicit, users are motivated to converge not only on the entities/concepts/data themselves, but also on the most effective ways to describe and reference these entities/concepts/data. This creates an incentive for users to reach fractal consensus on data structures, from individual Atoms to complex nested Triples.

By integrating these economic principles, Intuition not only secures the system against malicious attacks but also promotes a healthy, self-regulating ecosystem where users are rewarded for their contributions to the integrity and value of the data.

8.3.5 State Interpretations

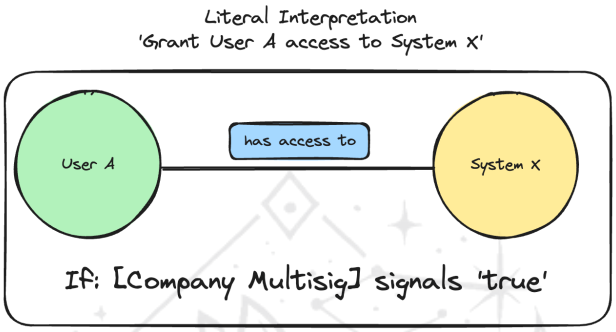
By implementing the aforementioned mechanisms, we achieve a state that can be interpreted in an almost limitless number of ways. Intuition deliberately avoids enforcing any specific interpretation of the data, aligning with its core principle of avoiding "truth lock-in" or the imposition of a singular perspective. The Intuition Protocol is designed to remain completely neutral regarding the interpretation of state and signal. Nevertheless, it is crucial to discuss the topic of interpretation within the Intuition system to provide an initial understanding of the various methods and perspectives that users might explore when analyzing the system's state.

Literal interpretations In the Intuition ecosystem, literal interpretations are explicit, structured expressions designed to facilitate coordinated, higher-order applications of its discrete state. These interpretations provide a foundation for a cohesive and interoperable framework, enabling various stakeholders to understand and utilize the system's data explicitly. By achieving consensus on how specific concepts should be expressed and interpreted, the ecosystem can develop a composable system of expression and logic, similar to programming languages.

Archived copy · cryp2nova.com

For instance, consider implementing an access control mechanism using the Intuition state. An implementor might use a specific Atom, defined as "has access to," as the Predicate in a Triple structure. The literal interpretation might state: if [Company's Multisig] attests to this Triple being True, this signifies that the Subject of the Triple has access to the Object—in this case, System X. This state can be used by the implementor to provision access to users of System X.

By publishing this literal interpretation, the implementor allows others to observe and utilize this interpretation for various purposes. For example, another system might use this information to grant User A access to System Y based on their access to System X, to adjust their loan-to-value ratio in a financial application, or to affect their reputation in a particular context.



The Intuition system facilitates the publication process of these literal interpretations, allowing stakeholders to register and share their interpretations as Atoms and/or Triples. By doing so, the system can be used recursively to create a registry of literal interpretations that promotes transparency and coordination. This registry enables the creation of programmatic languages on top of the Intuition protocol, leveraging the principles of discrete objects and their relationships to enforce logic and code.

Algorithms In the Intuition framework, algorithms function as tools to filter and interpret data, distinct from literal interpretations which resolve to deterministic logic. Given a permissionless environment where anyone can claim anything about anything, algorithms play a crucial role, enabling signal to be effectively distilled from the noise and allowing users to focus on the voices they trust.

Intuition rejects the idea of 'truth lock-in,' acknowledging that no single algorithm can be universally optimal. In response, Intuition promotes a diverse and permissionless ecosystem of algorithms that users and developers can select based on their specific requirements. This empowers users and developers to create, choose, and apply the most appropriate algorithms for their particular contexts. Such flexibility ensures that data filtering and interpretation can be customized to meet varied needs, thereby enhancing the overall utility and effectiveness of the Intuition framework.

This approach contrasts sharply with the current internet landscape, where platform interactions often necessitate accepting a pre-set, opaque algorithm. Intuition envisions decoupling algorithms from applications, allowing individuals to use their preferred algorithms across different platforms - a flexibility made possible through interoperable and composable data.

For instance, consider an algorithm that weights and filters data based on social graphs. In this model, a user who is one degree of separation away from the observer might have their signal weighted at 100%; at two degrees away, at 80%; and at three degrees away, at 60%. This allows for nuanced data interpretation based on social proximity.

Reality Tunnels By decoupling each element of the data filtering process, we unlock the potential to recombine these elements in novel and innovative ways. Within the Intuition framework, these combinations are known as "Reality Tunnels." A Reality Tunnel typically includes a mix of literal interpretations and algorithms, but it can also incorporate other relevant components essential for data filtering, weighting, and sense-making.

To illustrate, consider the creation of a 'Trust Graph' using specific Triple structures. For instance, a Triple might be formatted as '[Subject] [in trust graph] [Vitalik's Web3 Trust Graph].' This Trust Graph could assign different users different weights, explicitly signaled by a particular curator, to facilitate the weighting and filtering of data. When this Trust Graph is combined with an algorithm such as EigenTrust, it can

Archived copy · cryp2nova.com

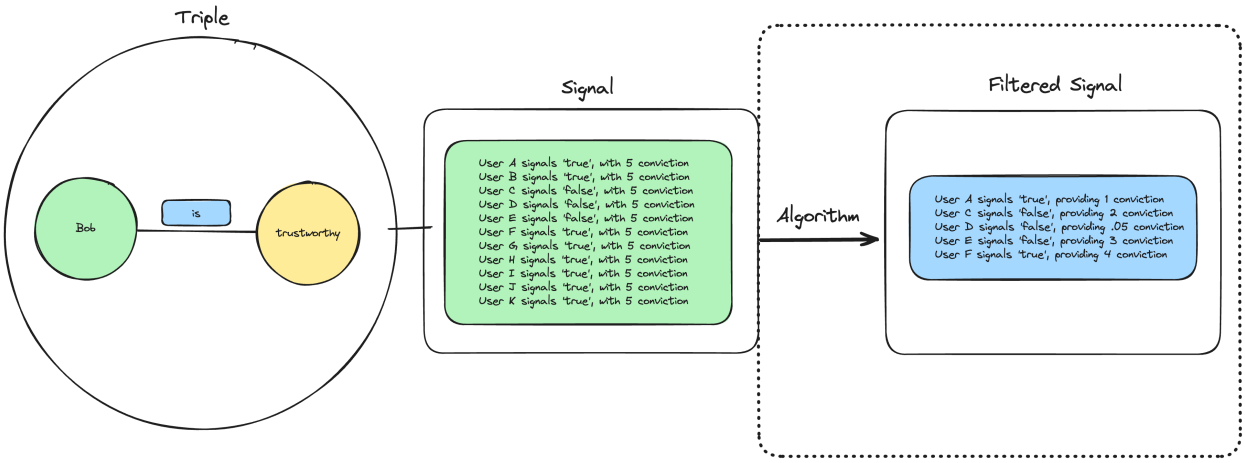


Figure 14: Data filtered through an algorithm, helping to distill the signal from the noise.

be applied to a relevant context—like a portion of the knowledge graph pertaining to Web3 topics. This integrated viewpoint or "lens" is referred to as a Reality Tunnel.

The concept of Reality Tunnels also allows users to switch between different perspectives. Imagine engaging in a debate and having the ability to view the data from your opponent's perspective to understand their reasoning. Currently, most platforms restrict users to a single "reality tunnel," shaped by their social graph and a specific platform's algorithm. However, if users could toggle between different social graphs and apply various open-source algorithms, they would gain access to diverse viewpoints and a more comprehensive understanding of the data and the world around them. This flexibility would enrich user experience by providing multiple angles on the same information, fostering better-informed discussions and decisions.

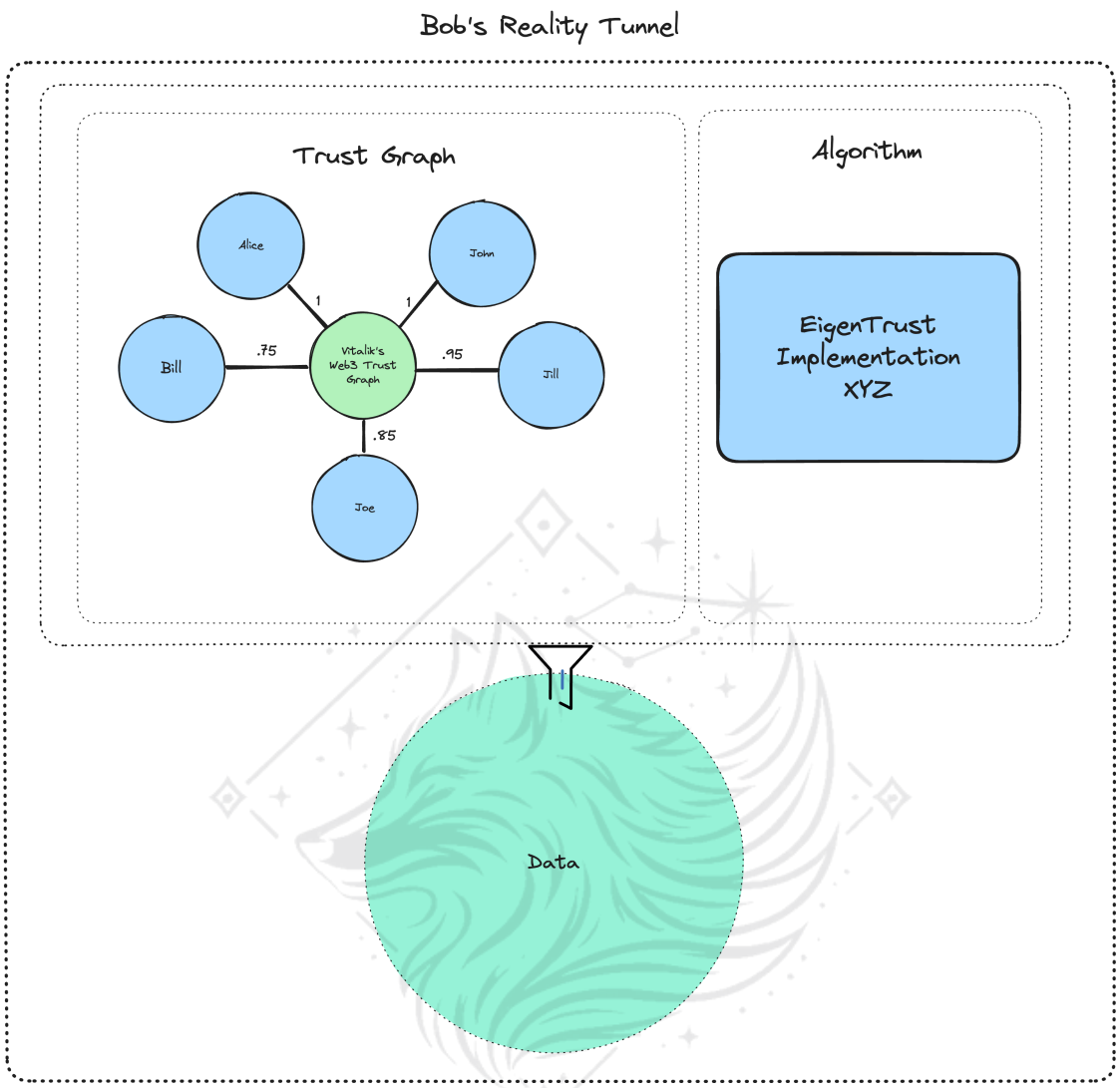
8.3.6 Intuition in Practice

The introduction of Intuition's core primitives lays a robust foundation for constructing a system that fosters a trustful interaction layer for the decentralized web. These seemingly basic primitives enable a wide range of powerful functionalities, transforming how we manage identities, data, and trust online.

To illustrate this, consider, once again, the experience of buying a product on Amazon. With Intuition's primitives, this process can be reimagined in a decentralized, trustless manner:

1. **Atoms and Triples**
   (a) Every user, product, review, and transaction can be represented as discrete objects (Atoms) and linked through relationships (Triples). For instance, a Triple could link a product (Atom) to a review (Atom) through a relationship like "hasReview."
2. **Signal**
   (a) Each review can be evaluated for credibility using the Signal primitive. Reviews and Signals from verified purchasers or highly reputable users can carry more weight, helping users discern trustworthy feedback from potentially fraudulent reviews.
3. **Fees, Economics, and Incentives**
   (a) Users are encouraged to express themselves, and reviewers are incentivized to provide honest and detailed feedback. Users earn money for their valuable data contributions, and their reputation becomes cross-contextual, increasing its significance beyond a single platform. For example, a user's status as a trusted reviewer on Amazon could serve as a valuable reputation data point in other contexts, such as securing better loan-to-value ratios in decentralized finance (DeFi) or enhancing the ability to obtain a loan. This cross-contextual reputation system contrasts with Amazon's current reviewer reputation, which offers no tangible rewards.
   (b) Additionally, users might be more inclined to attest to useful information about products on Amazon because their claims can be easily seen by the people they care about, thanks to portable social and trust graphs. Unlike the current Amazon platform, which lacks a friends

Archived copy · cryp2nova.com



list, Intuition allows users to take their singular social graph or a set of trust graphs with them anywhere they go. This portability means that the review of one trusted individual in a specific context could hold more weight than numerous anonymous reviews. The ability to leverage these portable social and trust graphs ensures that valuable insights from trusted sources are prioritized, further enhancing the reliability and utility of the data within the ecosystem.

4. **Interpretations**

   (a) The listing of a product on a marketplace such as Amazon can be represented as a literal interpretation. For instance, adding a product to a marketplace can be as straightforward as creating a Triple like [Product] [listedOn] [Amazon]. Expanding on this concept, various stakeholders can publish their interpretations of product reviews. For example, a company might aggregate all reviews and provide a summary score, while an independent consumer protection group could highlight reviews mentioning safety concerns.

5. **Algorithms**

   (a) Users can choose from various algorithms to filter and sort reviews based on their preferences. For instance, an algorithm can prioritize reviews from users with similar purchase histories or highlight reviews that mention specific product features.

6. **Reality Tunnel**

Archived copy · cryp2nova.com

(a) Users can compose together interpretations and algorithms to create curated 'views' of data, allowing them to find the voices they trust among thousands of anonymous voices.

7. **Portable Identity and Data**

(a) Identities and data become universal, and can be referenced and integrated anywhere across the web. Users can see a product's aggregated reviews across Amazon, Facebook Marketplace, Craigslist, or eBay, provided the same canonical identifier for the products is used in each context. And, even if Amazon were to shut down, users' data and lists of favorites would still exist, ensuring continuity and control over their digital interactions.

By integrating these primitives into contexts and interactions that cannot yet be fully 'trustless,' Intuition establishes a decentralized trust layer. This layer allows users to interact with confidence, knowing that the information they rely on is transparent, verifiable, and free from centralized manipulation. For instance, when buying a product, users can access a wealth of credible reviews, filtered and presented according to their preferences, all while maintaining control over their data and identities. By leveraging these tools, we can build a more trustworthy and user-centric digital ecosystem, addressing many of the inherent flaws in the current Web2 trust stack and paving the way for a more decentralized and equitable internet.

8.4 Design Decision Rationale

Having introduced the core primitives underpinning the Intuition system, before we transition to a more detailed examination and implementation details, it is imperative to delve deeper into the rationale behind these design decisions. By exploring the reasoning and guiding principles that informed the creation of these primitives, we can better appreciate their significance and the critical role they play in addressing contemporary challenges in digital trust.

8.4.1 The Vision: A More Semantic Web

In our pursuit of a trustful interaction layer, it is evident that building trust requires more comprehensive and reliable agent-centric information. The vision of a semantic web is central to achieving this goal. By ensuring that data is not only abundant but also structured and accessible, we can foster an environment where trust can flourish through informed decision-making.

To illustrate the vision of a more semantic web, consider the process of adding notes about a book to a reading list. Typically, this might involve jotting down the book title, the author, and perhaps some additional information in raw, unstructured text. Alternatively, one might paste the URL of the book from Amazon, which provides Amazon's link, data, and reviews. However, this approach restricts access to the data of a single platform, rather than leveraging the entire internet's wealth of information.

Imagine if this book had a unique, globally persistent, canonical digital identifier that could be referenced universally and directly. Using this identifier, it would be possible to instantly access all related data from across the web—ratings, reviews, purchase links, and more—regardless of the platform where the data resides. This identifier would serve as a unified reference point, aggregating information from multiple sources, thus providing a comprehensive view of the book. This would transcend Amazon's perspective, allowing access to reviews from Goodreads, purchasing options from various retailers, academic critiques, related articles, and even social media discussions.

Additionally, any data contributed about this book—such as personal notes, reviews, or tags—would be easily discoverable by others, enriching the global dataset. When annotating the book with thoughts or adding tags for easier referencing, these contributions become part of the shared knowledge pool. Other users, regardless of where they are on the web, can benefit from these inputs, just as they contribute their own.

Standardizing the structure of data about the book ensures consistency and interoperability across platforms. For instance, reviews can be categorized by sentiment, ratings can follow a universal scale, and purchase links can be formatted uniformly. This standardization allows for seamless integration and comparison of data from various sources, making it easier for users to interpret and utilize the information.

Incentivizing more and better expressions is also crucial. In this system, users should be encouraged to contribute high-quality data. Detailed and insightful reviews, comprehensive annotations, and accurate tagging are all examples of contributions that might be rewarded. This creates a virtuous cycle where the richness and reliability of the dataset continually improve as more users participate and contribute.

Archived copy · cryp2nova.com

This vision encompasses a more decentralized, semantic web, where data is seamlessly aggregated and accessible through universally recognized identifiers. Such a system fosters a dynamic and interconnected information ecosystem, vastly improving the efficiency and richness of digital interactions. By transcending the silos of individual platforms, we move towards a unified digital space where information flows freely and is easily accessible to all, ultimately enhancing the ability to find, share, and build upon knowledge.

The Challenge: Achieving Consensus In an entirely permissionless environment, where new data structures, schemas, formats, standards, and identifiers can be created and leveraged without permission, coordination is a complex challenge. The decentralized nature of the web aligns with the core principle of avoiding any single authority. Instead, consensus must emerge organically from the community, reflecting the diverse and often conflicting interests within it. This decentralized approach is crucial to maintaining the openness and democratic nature of the system.

In traditional systems, a centralized authority might impose standards and ensure adherence. For example, the International Standard Book Number (ISBN) system is centrally managed, ensuring that every published book has a unique identifier. However, relying on a singular authority to enforce such standards contradicts the ethos of decentralization. Centralization places an entity in a position of extreme power, which goes against the principles of promoting openness and avoiding monopolistic control.

Therefore, it is imperative that the process of reaching consensus be more democratic and community-driven. This involves the collective participation of users, developers, and stakeholders who contribute to and maintain the system. This approach encourages diversity and inclusivity, allowing for a broader range of perspectives and innovations. However, it also means that agreement on standards and identifiers can be slow and contentious, requiring extensive collaboration and negotiation.

To alleviate the coordination issues around achieving decentralized social consensus, mechanisms to facilitate collaboration and negotiation among a diverse set of participants must be put in place. Economic incentives, transparent governance models, and other consensus mechanisms play crucial roles in this process, driving participants towards mutually beneficial agreements while maintaining the decentralized nature of the system.

The Market-Driven Approach to Consensus The market-driven approach to consensus is a foundational principle within the cryptocurrency ecosystem. This method utilizes economic incentives and social consensus to establish standards for digital assets, contracts, or even entire blockchain networks. Mechanisms like Proof of Work (PoW) and Proof of Stake (PoS) are designed based on game-theoretic principles to ensure that participants' actions align with the network's best interests. These principles can extend beyond ledger states to include the establishment of canonical identifiers and the convergence on arbitrary industry standards.

For example, in the cryptocurrency realm, determining which PEPE coin should be considered the canonical version among thousands of identical deployments is primarily influenced by the market, given the absence of tangible fundamentals. The PEPE coin with the largest market capitalization becomes the recognized standard. This outcome is driven by the collective actions and decisions of the community, reflecting a preference for the most widely adopted version.

Prediction markets also demonstrate this market-driven consensus by converging on the correct answer as more data becomes available. Participants in these markets are economically incentivized to align their predictions with the most accurate outcomes, resulting in a consensus that mirrors the collective intelligence of the participants.

The ERC-20 token standard further illustrates this approach. Before its introduction, the Ethereum ecosystem lacked a uniform protocol for tokens, leading to fragmentation and interoperability issues. Developers and users recognized the benefits of adopting a common standard: interoperability, ease of integration, and enhanced security. By adhering to the ERC-20 standard, developers ensured that their tokens could seamlessly interact with various wallets, exchanges, and decentralized applications (dApps). Conversely, deploying a token that did not follow the ERC-20 standard would lead to significant challenges. Such a token might not be compatible with existing wallets, making it difficult for users to store or transfer it. It could also face integration issues with exchanges and dApps, limiting its usability and adoption. This lack of interoperability would create friction for both developers and users, discouraging the adoption of non-standard tokens.

In these examples, the power of incentives is evident: users naturally converge when it best serves their interests. The collective actions of community members, driven by their individual economic motivations,

Archived copy · cryp2nova.com

result in the organic selection of the most robust and valuable options. This market-driven approach ensures that the best solutions rise to prominence through organic consensus rather than imposed mandates.

The Role of Economic Incentives in Intuition Intuition leverages this market-driven approach by incorporating economic incentives to drive convergence on data structures, schemas, standards, and identifiers, as well as to encourage participation. Every action within the system incurs a nominal fee, similar to a gas cost in blockchain networks, which is used to grant fractional ownership of the data being interacted with and to compensate all other current owners. This mechanism ensures that participants are financially motivated to use and support canonical identifiers and standardized methods of expression, as they benefit from future interactions involving these elements.

For example, when a user makes a claim about a concept or entity, they gain fractional ownership of that claim and its associated data. Subsequent interactions that reference this data will generate rewards for all those who have previously engaged with it, thus incentivizing the use of widely accepted and recognized identifiers and standardized expressions. This alignment of individual economic interests with the collective goal of creating a cohesive and interoperable system is central to Intuition's design.

By adopting this market-driven approach, Intuition ensures that the most effective and reliable data structures, schemas, standards, and identifiers naturally gain prominence through community consensus rather than top-down directives. This system encourages the adoption of standardized identifiers and data structures, reducing fragmentation and enhancing interoperability across the digital landscape.

Furthermore, the economic incentives within Intuition create a dynamic and adaptable ecosystem capable of evolving in response to changing needs and challenges. As participants continuously interact with and contribute to the system, they collectively shape and refine the standards and practices that define the ecosystem. This is a significant departure from more centralized solutions, such as schema.org, which rely on predefined schemas and centralized control over data standards. Intuition's decentralized and incentive-driven model allows for a more flexible and responsive approach. As new types of data emerge and the community's needs evolve, participants can propose and adopt new standards organically. Economic incentives ensure that the most useful and widely accepted standards are adopted, while less effective ones are naturally phased out. This adaptability is crucial in a rapidly changing digital landscape where new technologies and use cases are constantly emerging.

Reducing Fragmentation & Solving the Problem of Folksonomies The concept of community-driven data structuring, exemplified by folksonomies, is not new. Folksonomies are user-generated systems for classifying and organizing information, that often lead to significant fragmentation. Unlike structured and hierarchical taxonomies, folksonomies allow individuals to use their own terms and descriptions for the same concepts. While this flexibility can be beneficial for personal organization, it frequently results in varied tags or labels being applied to the same item, creating a fragmented data landscape that is difficult to reconcile.

For instance, in a folksonomy, one user might tag an article about climate change with "global warming," another might use "climate crisis," and yet another might simply tag it "environment." Although all these tags refer to the same overarching topic, the lack of standardized labeling leads to scattered information, making it challenging to aggregate and analyze data comprehensively.

Intuition addresses this problem by incentivizing convergence on popular choices. By employing economic incentives, Intuition encourages users to adopt and promote canonical identifiers and descriptions. Every interaction within the system, such as tagging or classifying an entity, involves a small fee that contributes to fractional ownership of the data being interacted with. Users are motivated to use established identifiers because doing so increases their potential for economic rewards from future interactions.

This economic model promotes a more unified and coherent data structure by minimizing the fragmentation inherent in folksonomies. When users converge on standardized methods of expression - a concept which can be likened to the concept of language - it becomes easier to aggregate, query, and analyze data. The result is a more organized and accessible information ecosystem.

For example, if multiple users are tagging articles about climate change, they are incentivized to use the most popular and widely accepted tag, such as "climate change," rather than creating new or slightly different tags. This convergence reduces the scattering of related information and enhances the overall usability of the data.

Archived copy · cryp2nova.com

Intuition's economic incentives naturally create a token-curated registry (TCR) for expression, composed of TCRs for identifiers, schemas, formats, and standards. As users interact with and endorse specific identifiers and data structures, they gain ownership in these entities. This ownership makes the most useful and accepted identifiers and frameworks more easily discoverable and widely adopted, guiding the community towards standardized terms and improving the overall coherence and utility of the data.

Keynesian Beauty Contest in Intuition The Keynesian Beauty Contest principle is central to how Intuition fosters social consensus. In economics, a Keynesian Beauty Contest is a scenario where participants are rewarded for choosing options they believe others will choose, rather than their personal preferences. This concept is applied to Intuition's selection of identifiers and modes of expression, ensuring that the most popular and widely accepted options become canonical.

Application in Identifier and Description Selection

Judgment Based on Popularity In a Keynesian Beauty Contest, participants aim to predict the most popular choices among all participants. This method has been shown to be highly effective in reaching social consensus, as it aligns individual incentives with collective preferences. The principle was first introduced by John Maynard Keynes in his 1936 book "The General Theory of Employment, Interest, and Money," where he described a newspaper beauty contest in which participants were asked to choose the most popular faces rather than their personal favorites.

In Intuition, this concept translates to users being incentivized to choose identifiers and descriptions they believe will be widely adopted by others. This ensures that the most useful and accurate representations gain prominence. For instance, if a majority of users prefer the identifier [New York City] over [NYC] or [NY], the system will naturally converge on [New York City] as the canonical identifier.

Evidence of Effectiveness The effectiveness of the Keynesian Beauty Contest in predicting popular choices and achieving consensus has been demonstrated in various studies and real-world applications:

1. **Experimental Economics**: Studies have shown that participants in Keynesian Beauty Contest experiments often converge on the same choices, reflecting a strong predictive ability about the preferences of others. For example, in an experiment conducted by Nagel (1995), participants were asked to choose a number between 0 and 100, with the goal of selecting the number closest to two-thirds of the average choice. Over multiple rounds, participants quickly learned to anticipate others' choices, leading to convergence around the predicted equilibrium.
2. **Prediction Markets**: Prediction markets, which operate on similar principles to Keynesian Beauty Contests, have been shown to accurately forecast outcomes in various domains, including elections, sports, and financial markets. These markets reward participants for correctly predicting popular outcomes, and their accuracy is well-documented. For instance, a study by Berg, Forsythe, Nelson, and Rietz (2008) found that prediction markets outperformed traditional polling methods in forecasting the results of the U.S. presidential elections.
3. **Crowdsourcing and Consensus Mechanisms**: Platforms like Wikipedia and Stack Overflow leverage similar consensus mechanisms to ensure the accuracy and reliability of information. Contributors are incentivized to align their contributions with the community's expectations, leading to high-quality, consensus-driven content. Research by Kittur and Kraut (2008) highlighted the effectiveness of Wikipedia's collaborative model in achieving high information quality through collective intelligence.

Practical Example in Intuition Imagine users need to describe a widely known concept such as "Machine Learning." Multiple identifiers could exist: [ML], [MachineLearning], [AI], [ArtificialIntelligence]. Through the Keynesian Beauty Contest principle, users are incentivized to converge on the identifier they believe will be most widely adopted, and not necessarily the one they personally prefer. Over time, economic incentives may drive the majority to use [Machine Learning] over the other options, reducing fragmentation and enhancing data consistency.

For instance:

- Users making the statement [Machine Learning] [is] [a branch of AI] would prefer to use the identifier [Machine Learning] over [ML] to maximize their economic rewards from future interactions involving this statement.

Archived copy · cryp2nova.com

- As more users adopt [Machine Learning], the identifier becomes the canonical choice, and those who initially used it are rewarded economically, reinforcing its status.

This concept extends to Triples as well. In the previous example, [is] might not be the most explicit Predicate. A user might instead choose a more precise predicate such as [is a subset of]. Users are incentivized to converge on the most explicit and precise representations of data, as greater specificity enhances discoverability. Improved discoverability increases relevancy, which in turn amplifies the potential for economic rewards.

8.4.2 A Language Protocol for Digital Information Interoperability

With this, Intuition facilitates consensus on a common language across the web, guided by game-theoretic economic incentives. Historically, efforts to facilitate peer-to-peer interactions have concentrated on the lower levels of the internet stack, such as the transfer of data packets and ensuring network connectivity. Protocols like TCP/IP, HTTP, and DNS have established robust foundations for data transmission, addressing issues of reliability, routing, and domain naming, respectively. These foundational layers have been crucial in enabling the global, decentralized network we now call the Internet.

However, while these lower layers have been adequately addressed, allowing for efficient and reliable data transfer, the higher levels of the stack—specifically those involving data semantics and interoperability—remain fragmented and inconsistent. Traditional network protocols ensure that data can be transmitted from one point to another, but they do not address the interpretation, standardization, and meaningful integration of that data.

Intuition's framework represents a paradigm shift by focusing on standardizing the higher levels of the stack. It introduces a universal language protocol for digital information interoperability, addressing an unfulfilled need in the current internet infrastructure. By promoting consensus through economic incentives, Intuition ensures that data is not only transmitted but also seamlessly integrated and understood across different platforms and applications.

Moreover, the implementation of such a system has only recently become viable. With reliable data transmission and connectivity now largely a solved problem, attention can be turned to enhancing the quality and interoperability of the data itself. With the emergence of blockchain technology and trustless decentralized networks, new economic models and incentive structures that were not previously possible have been unlocked, allowing for the game theoretic mechanisms frequently employed in the blockchain ecosystem to be applied to higher-order consensus.

8.5 Primitives: In-Depth Analysis and A Rudimentary Implementation

With a high-level overview of Intuition established, we can examine how the Intuition protocol may be implemented in practice, highlighting its feasibility. In this section, we will explore a preliminary EVM-based implementation.

8.5.1 Atoms

Atom: *Intuition's atomic unit of knowledge. Atoms can be used to represent Subjects, Predicates, Objects, and Triples. All Triples are a composition of Atoms, and Triples can be used as Atoms in other Triples.*

In the Intuition system, Atoms function as the building blocks through which all higher-complexity structures are formed. The terminology highlights the fundamental role these identifiers play - just as atoms combine to form molecules, these Atoms can be composed into higher-order arrangements, enabling the deterministic and semantic organization of complex data.

The goal of the concept of Atoms is to achieve consensus around unique, globally persistent, decentralized digital identifiers for all things. Achieving consensus is essential for consistently and meaningfully referencing ***things of all types***—people, places, words, products, concepts, pieces of arbitrary data, etc.—universally across the web.

Atom Structure In the context of Intuition, an Atom represents any discrete entity, concept, or piece of data. The objective of Atoms is to assign a decentralized identifier to every conceivable discrete ***thing***. To achieve this, each Atom should possess at least three unique attributes, each contributing to essential functionality:

Archived copy · cryp2nova.com

1. **Atom Data**: Atom Data provides a detailed description of the Atom, enabling the clear identification of the concept or entity the Atom is meant to represent. This data can encompass any information of any format. This flexibility allows for the representation of data of any granularity, from general concepts such as a word, formula, or piece of code, to people or organizations. It is recommended that heavy Atom Data be stored off-chain, preferably via a decentralized data storage solution such as IPFS, with only a URI pointing to this data stored on-chain.
2. **Atom Wallet**: Each Atom has an associated Atom Wallet, which is meant to provide the Atom, or the rightful controller of the Atom, with agency over its identity. Any 'wallet' that is capable of handling controllership of the Atom is acceptable. Each Atom Wallet is initially controlled by the Atom Warden - a smart contract that manages all Atom Wallets - unless/until it is 'recovered' by an entity who can prove rightful ownership over the Atom (recovery methods will be explored later).
3. **Atom Vault**: An Atom Vault enables users to manipulate their balance with respect to each Atom by depositing tokens, thereby signaling the Atom's relevance. The total value locked (TVL) within an Atom Vault acts as a metric of the Atom's acceptance and importance within the system. Although any mechanism capable of trustlessly managing the tracking of balances can serve this purpose effectively, the implementation discussed here will involve vaults adhering to patterns akin to those of the ERC-4626 Tokenized Vault Standard to achieve this functionality.

Atom Data Atom Data provides a detailed description of the concept or entity represented by an Atom, ensuring its clear and distinct identification and referenceability within the Intuition system. This data can reside in any location or format, adhering to any schemas - though, naturally, some schemas may be more supported than others. Although an `atomURI` may be any arbitrary URI that points to any data, there is a strong preference for storing Atom Data in off-chain verifiable data registries such as IPFS (InterPlanetary File System). Utilizing these platforms offers significant advantages, including immutability and persistence, which are crucial for maintaining data integrity, availability, and persistence. URIs pointing to this data, such as IPFS Content Identifiers (CIDs), should be stored on-chain as `atomURIs`, ensuring that the data remains easily accessible and verifiable.

When linking to centralized data, there is a potential risk of data loss or alteration, as these sources may not offer the same level of permanence and verifiability as decentralized storage solutions. To mitigate these risks and ensure the persistence of critical data, it is advisable to take a snapshot of the Web2 data and store it on a verifiable data registry. This snapshot captures the state of the data at a specific point in time, preserving its integrity and providing a stable reference that can be reliably accessed in the future.

Transforming data into a more compatible format for easier consumption within Intuition is also important. This transformation process can involve standardizing the data schema, enriching the metadata, or converting the data into optimally compatible formats. For example, a Tweet's content and metadata can be captured, converted into a standardized 'social post' format, and stored on IPFS, with the resulting CID linked as the `atomURI`.

Because any data can be referenced by an Atom, encrypted data can also be referenced, allowing the use of any arbitrary encryption scheme to ensure data privacy. Although the utility of encrypted data may be limited by its inaccessibility, Intuition facilitates the discoverability of such data. For instance, a user may have sensitive, encrypted information such as health records or personal notes stored on their device or within an Identity Hub. The user can create an Atom that references this encrypted data and attach it to their identity using a Semantic Triple. For example, a triple like `{[Person] [health records] [arbitrary encrypted data]}` would make the data more easily discoverable and requestable by authorized parties, such as healthcare providers, as these parties would be able to query for `{[Person] [health records]}`. This capability enhances the accessibility and utility of encrypted data within a secure and privacy-respecting framework.

Atom Wallet Each Atom within the Intuition system is equipped with an Atom Wallet, providing the Atom with agency over its identity. This wallet acts as the controller of the Atom, initially managed by Intuition's Atom Warden—a specialized smart contract designed to facilitate the recovery of Atom Wallets. The recovery mechanism allows individuals who can demonstrate rightful ownership of the concept represented by an Atom to claim, or 'recover' control of, that Atom's wallet.

A parallel can be drawn to the platform Yelp in the Web2 environment. On Yelp, users can create profiles and post claims about restaurants before the establishments themselves have joined the platform. Once a restaurant registers on Yelp, it can claim and manage its profile, thereby gaining control over its digital

Archived copy · cryp2nova.com

identity. Similarly, in the Intuition system, users can create Atoms for any concept, and rightful owners can later gain control over these Atoms upon proving their legitimate ownership.

One straightforward example of a recovery method involves verifying ownership of an Ethereum address. If the `atomURI` of an Atom corresponds to an Ethereum address, the recovery process can confirm if the `msg.sender` matches the referenced address, using a method like `ecrecover` which allows for the recovery of a public key from a given signature. If there is a match, the Atom Warden would be authorized to transfer control of the Atom Wallet to the rightful owner. This method ensures that the true owner gains sovereignty over the Atom, enhancing the security and integrity of the decentralized identity system.

This recovery process is more straightforward for some items than others, necessitating the introduction of new recovery methods for different Atom Types over time. This iterative development will ensure robust and flexible mechanisms for the decentralized management of digital identities within the Intuition framework.

It is also recommended that the `CREATE2` opcode be employed to instantiate wallets in advance of recovery, which can significantly reduce gas costs. By leveraging `CREATE2`, wallet addresses can be deterministically precomputed and deployed only when a transfer of ownership is necessary. This approach ensures that wallet creation is efficient and cost-effective, avoiding the substantial gas fees that would typically associated with a deployment of a new smart contract wallet for every Atom.

Upon the creation of an Atom, its corresponding Atom Wallet is allocated a certain number of Shares within the Atom's Vault. Consequently, as interactions with the Atom occur, the Atom Wallet accrues a portion of the fee revenue generated. This mechanism serves as an economic incentive for individuals to 'recover' the Atom Wallet for Atoms they can substantiate rightful ownership of. If the gas costs associated with deploying the smart contract wallet are less than the accumulated ETH within the Atom Wallet, it becomes economically advantageous to claim the Atom Wallet. This incentivization structure ensures that rightful owners are motivated to assert control over their respective Atoms.

Atom Vault A notable attribute of Atoms is the ability of users to manipulate their balances with respect to each Atom, reflecting users' engagement and perceived relevance of each Atom. This capability enables the creation of a ranked list of Atoms based on relevance and usage, facilitating the discovery and utilization of the most pertinent Atoms for various purposes.

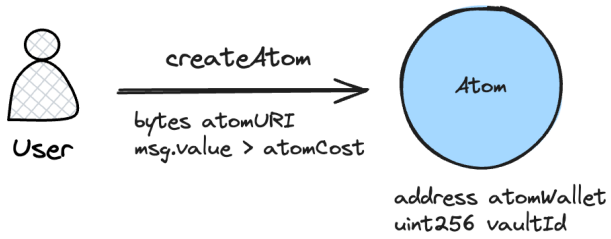
To accomplish this, an Atom Vault enables users to deposit tokens into an Atom, thereby signaling its relevance and support within the system. Users can make deposits directly into Atom Vaults, and programmatically make deposits into Atom Vaults when interacting with Triples that include the Atom as one of their constituent elements. Our discussed implementation of Vaults adopts the ERC-4626 standard, although various alternative methods may be utilized to achieve this functionality.

Depositing tokens into Atom Vaults serves multiple purposes. Primarily, it signals the relevance and support of an Atom. When users deposit tokens into an Atom Vault, they effectively endorse the Atom, indicating their belief in its value within the community. This endorsement is driven by economic incentives, as users can benefit from having a balance in Atoms that are frequently interacted with. Consequently, users are motivated to support Atoms they believe will gain traction and widespread acceptance. As each Atom's popularity and acceptance grow, so does the potential for economic rewards for its supporters.

The Total Value Locked (TVL) in an Atom Vault serves as a quantitative measure of the Atom's acceptance and relevance within the system. A higher TVL indicates greater community support and acceptance, providing a clear signal to other users about which Atoms are considered canonical for the concepts they represent. This TVL not only signifies support but also drives further interaction and engagement within the Intuition network.

Additionally, users deposit tokens into Atom Vaults indirectly through interactions with Triples that include the Atoms. Triples are semantic structures that describe relationships between Atoms, and depositing tokens into Triples automatically results in deposits into the associated Atoms' Vaults. This interconnected system ensures that support for individual Atoms is reflected through various interactions within the Intuition network. The cumulative effect of these deposits creates a Token Curated Registry (TCR) of all Atoms within the Intuition system, as curated by interaction and usage. This TCR functions as a decentralized, community-curated registry of identifiers for all things, continuously evolving based on the community's interactions and endorsements.

Archived copy · cryp2nova.com



Atom Creation & Usage To create an Atom on-chain, an `atomUri`, which can be any arbitrary bytes, must be provided. While any bytes are permissible as the `atomUri`, it is recommended that these bytes resolve to a URI referencing meaningful data.

The creation of an Atom requires a minimum payment, known as `atomCost`. This `atomCost` includes several fees:

1. **Atom Creation Fee**

`atomCreationFee`: An amount paid to the Intuition Protocol for the creation of an Atom. All 'protocol fees', or fees paid to the Intuition Protocol, may be likened to a 'gas cost' in any blockchain-based system. These protocol fees serve two primary purposes:

1. Aiding in the prevention of Sybil & DOS attacks
2. Ensuring the maintenance and upkeep of the system by imposing fees which outweigh the cost of computation and storage of each action
3. **Initial Wallet Deposit**

`walletInitialDeposit`: An amount deposited into the respective Atom's Vault on behalf of the `atomWallet`, granting the `atomWallet` Shares of its own Vault. The primary purpose of the `walletInitialDeposit` is to ensure that each `atomWallet` accumulates value as the Atom is interacted with, thereby incentivizing those who can prove rightful ownership over the Atom to claim the atomWallet. For instance, consider an Atom created for Restaurant A that has gained significant traction and activity. A portion of all fees paid will be allocated to the `atomWallet` due to the Shares purchased through the `walletInitialDeposit`. Consequently, over time, the bounty for Restaurant A (or its owner/team) to onboard to Intuition and 'recover' the atomWallet becomes economically attractive.

[resume]**Ghost Shares**

`minShare`: A fixed amount used to purchase 'ghost shares' in the vault for a neutral address (e.g., a protocol-controlled address or a zero address). This mechanism is designed to prevent inflation attacks and stabilize pricing when shares or assets approach zero value.

Atom Deposit on Creation

Should the amount provided by the Atom creator surpass the specified `atomCost`, the surplus is deposited into the Atom's Vault on behalf of the creator. This mechanism aids in preventing front-running and enables the Atom creator to acquire the initial shares of their newly-created Atom. Upon invocation of the `_depositOnVaultCreation` function to facilitate the purchase of shares, a `protocolDepositFee` is applied, representing a percentage of the deposited amount.

Share Price

When depositing in a Vault, the number of shares received is dictated by the current `sharePrice` of the Vault, which is determined by the bonding curve of the respective Vault. Any Vault may have any arbitrary bonding curve, an element of the system further explored in future sections.

A bonding curve is a mathematical concept used in tokenomics to define the relationship between the price of a token and its supply. It serves as a pricing mechanism that dynamically adjusts the price of a token based on the number of tokens in circulation or the total value locked within a system. In the context of Vaults, bonding curves are utilized to establish the `sharePrice`, influencing how many shares are received per unit of deposit and how they appreciate over time.

Archived copy · cryp2nova.com

Bonding curves can take various forms, but they all share some common principles:

1. **Formula-Based Pricing**: A bonding curve is typically defined by a mathematical formula, such as a linear, polynomial, or exponential equation, which dictates how the sharePrice changes with respect to the supply of shares or the amount of capital in the Vault.
- **Dynamic Adjustments**: As more capital is deposited into the Vault and more shares are issued, the bonding curve adjusts the sharePrice accordingly. Conversely, when capital is withdrawn and shares are burned, the sharePrice may decrease based on the curve's design.
- **Incentivizing Early Participation**: Bonding curves often reward early participants with lower entry prices. As the Vault grows and more capital is deposited, the sharePrice increases, providing an incentive for early investors.

Atom Structuring

The structuring of Atoms within the Intuition framework is guided by the principle of economic optimization. Given the economic bandwidth required for the creation of an Atom, it is economically advantageous to generate high-quality Atoms rather than suboptimal ones. Users are incentivized to ensure that the Atoms they create are maximally relevant and reusable to optimize their economic rewards.

Consider the concept of 'trustworthy'. If a user intends to express a statement involving this concept and finds no existing Atom that adequately captures it, the user is motivated to create a new Atom. In doing so, the user might adhere to established schemas such as the https://schema.org/DefinedTerm, incorporating as much pertinent data as possible. Additionally, the user might reference the concept 'trustworthy' within a lexical corpus like WordNet to enhance the Atom's utility across different languages.

While it is possible for the user to create an Atom that merely represents the raw string 'trustworthy', this approach would likely result in an Atom that is less useful to other users. Consequently, other participants may prefer to utilize more comprehensive Atoms. Therefore, it is in the best interest of system participants to create and converge on Atoms that effectively and optimally describe the intended concepts.

A Token Curated Registry of Atoms

With these mechanics in place, Intuition creates a global, permissionless, decentralized TCR of decentralized identities for all things—forming something akin to a universal, crowdsourced dictionary. This 'dictionary' - which can grow to encompass all entities, concepts, and data - serves as the foundation for expressing complex concepts.

As users create and interact with Atoms, they are economically motivated to produce and utilize Atoms that are highly relevant, reusable, and well-structured. Through the allocation of economic bandwidth and user engagement, Atoms that best represent concepts and meet the needs of the community will naturally rise to the top of the registry.

This TCR mechanism creates a dynamic and self-regulating system where the value of Atoms is continually assessed and validated by the collective actions of the users. The economic incentives ensure that participants are driven to contribute high-quality data, fostering an environment of continuous improvement and refinement. In this way, the Intuition system evolves into a comprehensive registry of all concepts, represented by Atoms, where the most effective and widely accepted representations are prominently featured.

8.5.2 Triples

While Atoms can be likened to individual words in a dictionary, Triples may be thought of as sentences that establish relationships between these words to express higher-order concepts. To maintain a coherent semantic structure across all fractals of the data, Intuition employs Semantic Triples, also known as RDF triples and often referred to here as 'Triples', for all higher-order expressions. Triples create discrete units of expression, facilitating precise representation and querying, and allowing for the construction of consensus mechanisms around expression standards.

[[cite: https://en.wikipedia.org/wiki/Semantic_triple]]

> A **semantic triple**, or **RDF triple** or simply **triple**, is the atomic data entity in the Resource Description Framework (RDF) data model.[1] As its name indicates, a triple is a sequence of three entities that codifies a statement about semantic data in the form of subject–predicate–object expressions (e.g., "Bob is 35", or "Bob knows John").

Archived copy · cryp2nova.com

> This format enables knowledge to be represented in a machine-readable way. Particularly, every part of an RDF triple is individually addressable via unique URIs'.
>
> Given this precise representation, semantic data can be unambiguously queried and reasoned about.
>
> The components of a triple, such as the statement "The sky has the color blue", consist of a subject ("the sky"), a predicate ("has the color"), and an object ("blue"). This is similar to the classical notation of an entity–attribute–value model within object-oriented design, where this example would be expressed as an entity (sky), an attribute (color) and a value (blue).
>
> From this basic structure, triples can be composed into more complex models, by using triples as objects or subjects of other triples—for example, `Mike` $\rightarrow$ *said* $\rightarrow$ (*triples* $\rightarrow$ *canbe* $\rightarrow$ *objects*).
>
> Given their particular, consistent structure, a collection of triples is often stored in purpose-built databases called triplestores.

In Intuition, a Triple's Subject, Predicate, and Object are each represented by an Atom. For example, a Triple might be `{[Alice] [is] [trustworthy]}`, where `[Alice]`, `[is]`, and `[trustworthy]` are all Atoms.

Because Atoms can represent any entity, concept, or data, an Atom may also represent a Triple. This allows Triples to be used as Atoms in other Triples, enabling the expression of arbitrarily complex statements in a standardized, semantic format.

Triple Structure

A Triple is formed by linking three Atoms in the following manner:

- **Subject:** Represents the entity or concept being described. For example, in the statement `{[Alice] [is] [trustworthy]}`, `[Alice]` is the subject.
- **Predicate:** Describes the relationship or attribute of the subject. In this example, `[is]` serves as the predicate, akin to the key in a key-value pair.
- **Object:** Denotes the value or characteristic attributed to the subject. Here, `[trustworthy]` is the object, akin to the value in a key-value pair.

Triple Metadata

Each Triple may also include metadata such as the creator, timestamp, and any additional contextual information. This metadata helps to ensure that the provenance and context of each statement are clear and verifiable.

Triple Vaults

Each Triple has two associated Vaults:

- **Positive Vault**: Used for signaling affirmation of the statement described by the Triple.
- **Negative Vault**: Used for signaling rejection of the statement described by the Triple.

While a Token Curated Registry (TCR) of Atoms allows for consensus around globally persistent canonical identifiers, a TCR of Triples allows for consensus around higher-order data standards and structures. This is useful in preventing data fragmentation and ensuring universal data usability. Unlike Atoms, where relevancy is the primary concern, Triples also demand consideration of the truthfulness of the statements they represent. Consequently, each Triple has two vaults: one for affirming the statement expressed by the Triple, and one for rejecting it, akin to a non-resolving prediction market for arbitrary data.

This dual-vault system facilitates consensus and dispute resolution by providing a clear method for signaling agreement or disagreement, helping to gauge community sentiment and resolve conflicts. Through the introduction of incentive mechanisms for convergence on specific Triples, Intuition promotes good data quality, consensus on data standards and structures, and the realization of a semantic web.

8.5.3 Example Scenario

Consider once again the Triple `{[Alice] [is] [trustworthy]}`. Users who 1) believe that this data structure is the appropriate way to express Alice's trustworthiness, and 2) agree that Alice is indeed trustworthy,

Archived copy · cryp2nova.com

can deposit tokens into the Positive Vault, thereby signaling their affirmation of the statement. Conversely, users who question Alice's trustworthiness can deposit tokens into the Negative Vault, indicating their rejection of the claim. The accumulation of tokens in either vault provides the community with a clear, quantifiable measure of collective sentiment regarding Alice's trustworthiness, backed by the collateral of the participants.

While 'depositing tokens into a Vault' may sound daunting in practice, this 'depositing' is meant to be abstracted away from the user. Thus, this process of claiming '[Alice] [is] [trustworthy]' may be as simple as hitting a thumbs up on an endorsement on a platform such as LinkedIn, or clicking an emoji reaction button on a social media platform such as Twitter.

Creating Triples

The process of creating a Semantic Triple necessitates the input of three fundamental components—Subject, Predicate, and Object—accompanied by a value that exceeds the specified `tripleCost`, akin to the `atomCost`. While any Atom can be designated as the Subject, Predicate, or Object, it is strongly recommended to adhere to proper Semantic Triple structure to ensure logical coherence and clarity.

To prevent the creation of duplicate Triples, each newly established Triple must possess a unique hash. This is essential for preventing fragmentation of sentiment and liquidity. This hash should be generated using a Secure Hash Algorithm such as `keccak256`, which is based on the concatenation of the URIs of the Subject, Predicate, and Object. In cases where a Triple's hash is not unique, participants can deposit tokens into one of the Triple's respective Vaults to signal either endorsement or rejection. The specifics of this signaling process will be elaborated in subsequent sections.

The `tripleCost` encompasses several components:

1. **Triple Creation Fee**

`tripleCreationFee`: An amount paid to the Intuition Protocol for the creation of a Triple. As previously mentioned, all 'protocol fees', or fees paid to the Intuition Protocol, may be likened to a 'gas cost' in any blockchain-based system - an essential component of any truly permissionless system.

[resume]**Atom Fraction**

`atomDepositFractionOnTripleCreation`: A fixed amount allocated to the Vaults of the constituent Atoms. When a Triple is created, there is an implicit signaling of support of the Atoms which comprise the Triple. As such, a fraction of the `tripleCost` is distributed to each of the Triple's respective Atom Vaults, rewarding the current shareholders of those Vaults.

[resume]**Ghost Shares**

`minShare`*2, used to purchase 'ghost shares' in each of the Triple's two Vaults. As mentioned in the Atom Creation section, this mechanism is designed to mitigate inflation attacks and stabilize pricing when shares or assets approach zero value.

Triple Deposit on Creation

When the value transferred during Triple creation exceeds the specified `tripleCost`, the surplus amount is deposited into the Triple's Positive Vault on behalf of the creator. This mechanism serves to prevent front-running and enables the Triple creator to acquire the initial shares of the newly created Triple. The function `_depositOnVaultCreation`, invoked to purchase these shares, incurs a `protocolDepositFee`, representing a percentage of the deposited amount, thus ensuring fair compensation for the protocol's operations.

Additionally, a portion of this deposit is allocated to each underlying Atom Vault associated with the Triple. This mechanic is introduced due to the fact that depositing into the Vault of a Triple that includes an Atom is a signal of an Atom's relevancy - which is a behavior expressed through depositing into an Atom Vault.

Share Price

Similar to Atoms, when depositing into the Vault of a Triple, the number of shares received is determined by the current `sharePrice` of the Vault, which is governed by the bonding curve specific to that Vault. As previously noted, any Vault can be associated with an arbitrary bonding curve, a feature of the system that will be explored in more detail in subsequent sections.

Given that any Vault can adopt any bonding curve, different bonding curves may be utilized for Triple Vaults as opposed to Atom Vaults, depending on the desired outcomes and behaviors in each scenario. This

Archived copy · cryp2nova.com

flexibility allows for the customization of economic dynamics to suit the unique requirements and goals of different types of Vaults within the Intuition system.

Structuring Triples

Proper structuring of Triples is fundamental to the efficacy of the Intuition system. Well-constructed Triples enable data to be easily indexed, queried, and discovered, enhancing the overall utility and accessibility of the system. Triple structuring primarily involves the standardized ordering of elements and the selection of appropriate Predicates.

Consider the scenario in which a user wishes to add a Book to a Book List. While there are numerous ways to express this relationship, let us examine two semantically correct approaches:

Book [inList] [Book List]

Book List [hasEntry] [Book]

In this example, the community may eventually converge on one standard expression over the other. Initial fragmentation within the Intuition system is anticipated as users experiment with various methods of expression. However, over time, consensus on preferred structures is likely to emerge.

The economic incentives embedded within the system play a crucial role in fostering this consensus. Users are rewarded for adopting Triple structures they believe will gain widespread acceptance, thereby aligning individual actions with the collective interest of the community. This incentivization mechanism ensures that the most effective and coherent Triple structures rise to prominence, facilitating a more organized and efficient data ecosystem.

A Token Curated Registry of Triples

With these mechanics in place, Intuition creates a global, permissionless, decentralized TCR of structured data, capable of expressing any arbitrary concept. In stark juxtaposition to the data structuring paradigm of the present, which oftentimes involves significant 'human' friction, the Intuition system provides guardrails for organic convergence on consensus data structures. With this, a self-sustaining system for the continual optimization of data structures is established, as users continually compete to structure semantic data in increasingly complex and expressive ways.

Atom and Triple Structuring Recommendations The semantic integrity of the Intuition system relies heavily on the community's adherence to proper structuring practices. To encourage this adherence, Intuition incorporates incentive mechanisms designed to promote best practices. However, these incentives alone are insufficient without the community's understanding of what constitutes 'best practices.'

In the nascent stages of Intuition, there is a heightened risk of the ecosystem generating suboptimal data due to a lack of structured guidance. Therefore, it is crucial to disseminate knowledge about proper structuring practices to ensure the creation of high-quality, semantically robust data, thereby safeguarding the system's overall efficacy and integrity.

Promoting Flatness for Scalability: Understanding the Power Set Problem

Although any concept, including arbitrarily higher-order and composite concepts, can be represented by an Atom, the Intuition system favors a "flat" data structure. This means that higher-order data structures should be composed through Triples wherever possible, rather than deeply nested Atoms. This approach minimizes the risk of data fragmentation and promotes a more coherent and easily navigable data structure.

To understand the reasoning behind this and its importance, we can examine the Power Set Problem and its applicability to data.

The power set of a set S is the set of all subsets of S, including the empty set and S itself. If S has n elements, the power set of S will have 2^n elements. Extrapolating this out to data, any expression can have this number of permeatations, when viewing each discrete piece of data as an element of S. This exponential growth illustrates the complexity that arises when dealing with numerous combinations in data structures.

The equation for the power set is often written as:

$$P(S) = \{A \mid A \subseteq S\}$$

Here, $P(S)$ denotes the power set of S, and A represents all possible subsets of S.

For example, if $S = \{1, 2, 3\}$:

Archived copy · cryp2nova.com

- The subsets are: $\{\}, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}$
- The power set $P(S)$ is $\{\{\}, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$

Consider a verifiable credential with a schema 'Profile' containing 25 fields, such as 'Name' and 'Age'. The number of possible field combinations is , resulting in 33,554,432 potential schemas. If we further take into account the permutations of each of those fields—such as 'firstName' and 'lastName' versus 'FullName'—the complexity grows exponentially. This exponential growth is a fundamental reason why the world's data is often irreconcilable, leading to significant annual expenditure of time, energy, and resources on data reconciliation efforts.

Implementing Flatness in Data Structuring

Intuition addresses these challenges by incentivizing 'flatness' in data structuring. Users are encouraged to create the most minimal and efficient schemas possible. This incentive is driven by the understanding that the profitability of data expressions in Intuition is directly proportional to the level of interaction they generate. Therefore, it becomes economically optimal to develop and utilize small, discrete, and reusable pieces of data, which can then be semantically composed in a manner that maximizes their reusability.

For instance, consider the process of attaching fields to an object and then associating that object with a subject. Suppose we have a subject "Author" and we want to attach information about a "Book" written by this author. Instead of creating a complex, nested schema, we would break down the information into minimal, flat structures:

1. Create an object for the "Book" with discrete fields:

   Book [title] [Book Title]

   Book [publishedDate] [Publication Date]

2. Attach the "Book" object to the "Author" subject:

   Author [hasWritten] [Book]

By structuring data in this flat, modular manner, where each field of a schema is represented as a Semantic Triple, the Power Set Problem is solved for through a reduction of the number of possible permutations to a linear rather than exponential equation. This reduction significantly simplifies the data structure and enhances its manageability and scalability.

Example of Flat Structuring

Consider a profile schema with five fields: Name, Bio, Image, Title, and Age. If users want to create variations of this schema, they might face exponential growth in potential schemas:

- User 1 might create a schema with Name, Bio, Image, Title.
- User 2 might create a schema with Name, Bio, Image, Age.

With five fields, there are 32 possible schemas. This paradigm requires extensive coordination and oftentimes leads to 'standards hell', where consensus is difficult to achieve, causing fragmentation and interoperability issues.

Instead, by expressing each field through a separate Semantic Triple, Intuition simplifies the structure:

```
[
  {
    "subject": "User A",
    "predicate": "Name",
    "object": "Object A"
  },
  {
    "subject": "User A",
```


Archived copy · cryp2nova.com

```
    "predicate": "Bio",
    "object": "Object B"
  },
  {
    "subject": "User A",
    "predicate": "Image",
    "object": "Object C"
  },
  {
    "subject": "User A",
    "predicate": "Title",
    "object": "Object D"
  },
  {
    "subject": "User A",
    "predicate": "Age",
    "object": "Object E"
  }
]
```

This approach eliminates the schema problem, making data more reconcilable, usable, and interoperable. In the example above, there are only 5 potential Triples that could exist representing this concept, assuming the same set of Atoms. By using 'consensus Atoms' to represent specific concepts and entities, and structuring data in the form of Semantic Triples, Intuition ensures that each piece of data has a clear, standardized meaning. Since each Atom has a definition, platforms across different contexts can rely on the same set of Triples to describe entities and their attributes, rather than needing to create and agree upon standard schemas. This leads to a significant reduction in data fragmentation and increases the interoperability of data across various systems.

Consider two different doctor's offices—Doctor's Office A and Doctor's Office B—both needing to store and share information about a patient named Bob. In a traditional system, each office might develop its own schema to store Bob's information, leading to potential discrepancies and difficulties in reconciling the data between the two systems.

Doctor's Office A might create a schema that includes fields like "FirstName" and "LastName," while Doctor's Office B might use "FullName." Similarly, one office might record Bob's age in a field named "PatientAge," while the other uses "AgeInYears." These differences in schema design can lead to significant challenges when attempting to merge or compare data across systems.

In contrast, Intuition's approach using semantic triples and Atoms helps to eliminate these issues. Both offices could use the same set of consensus Atoms and triples to record Bob's information, ensuring consistency and interoperability. Here's how it would work in practice:

Doctor's Office A wants to claim that the first name of User A is 'Bob'. They would use the Atom for "FirstName" as the Predicate of their triple, structured as follows:

```
{
  "subject": "User A",
  "predicate": "FirstName",
  "object": "Bob"
}
```

Doctor's Office B wants to claim that the first name of User A is 'Bob' and also that Bob's age is 32. They would use the same Triple for "FirstName", and an additional Triple for "Age", with the "Age" Atom inserted as the Predicate of the Triple:

```
{
  "subject": "User A",
  "predicate": "FirstName",
  "object": "Bob"
}
{
```


Archived copy · cryp2nova.com

```
  "subject": "User A",
  "predicate": "Age",
  "object": "32"
}
```

By using the same Atoms and Triples to express "Name" and "Age," both doctor's offices ensure that their data is structured in a consistent and interoperable manner. This consistency means that any platform or application interacting with this data can easily understand and reconcile it, regardless of its point of origination.

Optimal Data Flatness

While it is essential for data to be relatively 'flat' to facilitate ease of use and interoperability, overly flat data structures can lead to significant ambiguities. This concept is illustrated by what can be referred to as the "Father Father Problem", a term coined by Mr. John McClure of Intuition.

Consider an Atom, which is the fundamental unit of information in this context, represented solely by the string "father." Although this representation is maximally flat, it lacks the necessary context to discern its intended meaning. The term "father" could refer to a parental figure or a priest in the Christian church. Without additional context, the true meaning of this Atom remains unclear.

Ambiguity and Economic Incentives In an entirely flat data structure, where Atoms are maximally minimized, additional context would added through Triples (contextual data points). For example, in the 'Father Father Problem', a Triple could be created to add context, such as `{[Father Atom] [has definition] [parental father]}`. However, in an entirely permissionless environment, this method does not guarantee a consistent or deterministic definition. For instance, some users might use the Atom "father" to denote a parental father, while others might still use it to refer to a priest. This inconsistency introduces extreme ambiguity, making the data challenging to interpret accurately.

Moreover, such ambiguity can lead to unintended economic consequences. For example, if User A makes a claim `{[Bob] [is father of] [John]}` intending to express a parental relationship, they would receive shares of the Vault associated with the Atom [is father of]. If User B then makes a claim `{[Joe] [is father of] [Bill]]`, intending to express a religious relationship, User A would still be rewarded economically despite their data being entirely unrelated to User B's claim. This misalignment contradicts the goal of rewarding convergence and meaningful contributions.

Achieving Optimal Flatness To avoid these pitfalls, it is crucial to strike a balance in the flatness of data. While Intuition allows users the flexibility to structure Atoms as they see fit, it highly recommends the use of shallow-nested, generic schemas to define Atoms. This approach provides explicit clarity about what an Atom represents, reducing ambiguity and enhancing data reliability.

A standard generic schema might look like this:

```
{
  "genericSchema": {
    "name": "string",
    "description": "string",
    "url": "string",
    "image": "string"
  }
}
```

By incorporating a few "loosely immutable" fields, we can ensure a degree of certainty that the Atom accurately represents the intended concept, and that the core concept represented remains stable over time.

The Importance of Loosely Immutable Definitions

If an Atom's definition were solely derived from social consensus and claims, it could change unpredictably, leading to confusion and misrepresentation. For instance, if an Atom initially defined as "trustworthy" is later redefined as "liar" based on social consensus, historical claims would be misleading without considering the time context, complicating the system unnecessarily.

Archived copy · cryp2nova.com

"Loosely immutable" definitions mitigate this issue by providing stability while allowing for updates. The term "loosely" indicates that the definition can be changed, but such changes are deliberately challenging to implement. This ensures that users can trust that the definitions will not shift unpredictably.

To allow for necessary updates over time, some potential methods include:

1. Use Triples to update the Atom's definition.
2. Enable shareholders of an Atom to vote on updates to the Atom's off-chain data, creating fractal data DAOs for all concepts.

This balance ensures that while the definitions of Atoms can evolve, they do so in a controlled and deliberate manner, preserving the integrity and utility of the data.

8.5.4 Signaling

The concept of signaling in Intuition is decoupled from Triples, enabling many-to-one attestations/claims. This decoupling ensures that multiple participants can attest to the same statement without creating redundant data.

Signaling Mechanism

1. **Depositing Tokens**: Expression of Signal is achieved by depositing tokens into the Vault of the Atom or Triple. This act of depositing tokens serves as a Signal of the user's belief in the Atom/Triple's validity and/or relevance.
2. **Positive and Negative Vaults**: For Triples, participants have the option to deposit tokens into either the Positive Vault to affirm a claim, or the Negative Vault to reject it. This dual-vault system allows for a nuanced representation of consensus within the community.
3. **Economic Interpretation**: The state of balances within these Vaults reflects "who is saying what, and with what degree of conviction." This model enables the system to interpret data based on the number of participants supporting a claim, the economic bandwidth expended, and the reputation of each participant.

Example Signal

To articulate a statement within the Intuition system, participants deposit tokens into a Vault associated with a specific Triple. For example, if a participant wishes to assert that `{[Bob] [is] [trustworthy]}`, and this Triple already exists, they would express this sentiment by depositing tokens into the Positive Vault of the existing Triple, rather than by creating a new Triple.

With this, each Vault can exist in an infinite number of states based on participant deposits. For instance, a Vault could have 10 participants with a total value locked (TVL) of 10 ETH in the positive Vault, and 100 participants with a TVL of 5 ETH in the negative Vault. This state can be interpreted in many ways, based on several variables, such as:

1. The number of depositors in each vault
2. The reputation of each depositor, especially in the given context.
3. The economic bandwidth expended, in total and by each depositor, to support each claim.
4. The duration of the value locked by each participant.

Intuition itself remains neutral and does not assert what is true or false. Instead, it facilitates the generation of semantically interpretable states. Anyone can then build on this foundation to interpret the state in any way.

Independence and Correlation In the proposed implementation of Intuition, a Triple's Positive and Negative Vaults are economically uncorrelated - that is, activity in a Triple's Positive Vault will not impact activity in the Triple's Negative Vault. This is because, in a sense, these are two entirely separate claims. However, the activity does indirectly benefit both sides because they reference the same Atoms. Since these Atoms are utilized by participants in both the Positive and Negative Vaults, value is disseminated to both sides at the Atom level.

Archived copy · cryp2nova.com

8.5.5 Fees and Bonding Curves

In Intuition, bonding curves and fees play a pivotal role in determining the amount of assets a user can redeem from a Vault after depositing. When a user deposits assets into a Vault, they are issued Shares in return. These Shares represent the user's stake and can be redeemed for assets at any time. The price of these Shares may follow any bonding curve, though the intended behavior of the system is to reward current depositors whenever additional economic bandwidth is allocated to the respective Vault.

To ensure this behavior regardless of the bonding curve leveraged, the system implements a concept known as the Entry Fee (`entryFee`). The `entryFee` is a portion of a deposit that is distributed to all current Vault depositors. The system may also implement an optional Exit Fee `exitFee` on redemptions, providing a portion of redemptions to all current Vault depositors.

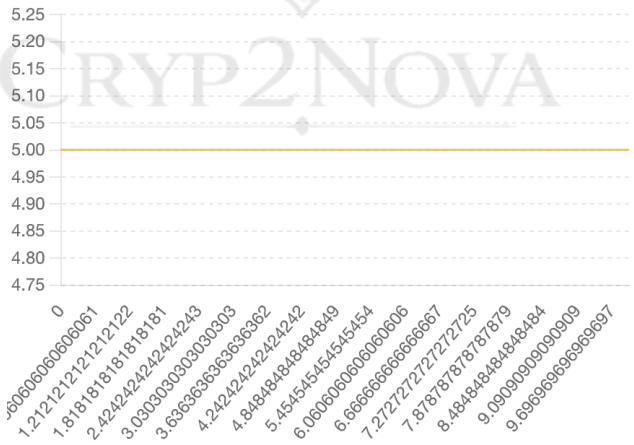
EntryFee Mechanism Entry Fee paid to all current shareholders to incentivize current holders

`entryFee` are `exitFee` are configurable parameters set by the protocol and can vary across different Vaults. The purpose of the these fees is to incentivize different behaviors and create various economic dynamics within the protocol. For instance, higher `entryFees` might discourage frequent trading, promoting longer-term holding, while lower `entryFees` might encourage more frequent interactions. By customizing the `entryFee` and `exitFee` for each Vault, the protocol can support a wide range of applications and user behaviors.

To streamline the process and minimize gas costs, `entryFees` and `exitFees` can be distributed to current Vault shareholders through an increase in Share price rather than direct payments. For example, when a user deposits assets and an `entryFee` is applied, the `entryFee` can increase the total assets in the Vault without increasing the total number of Shares. This mechanism effectively raises the share price, allowing existing depositors to redeem their Shares for a greater number of assets. Thus, the value of the entryFee is indirectly transferred to the current depositors.

Example Bonding Curves While `entryFees` and `exitFees` can encourage behavior to some extent, to accommodate the diversity of potential applications, it is recommended that a Bonding Curve Registry be implemented. This registry allows Vault creators to choose from a variety of predefined bonding curves when setting up a new Vault. The selected bonding curve will dictate the `sharePrice` curve of each Vault, and, consequently, the dynamics of share issuance and redemption for that Vault. To illustrate different scenarios benefiting from different bonding curves, we will explore some example curves:

Flat / Pro-Rata



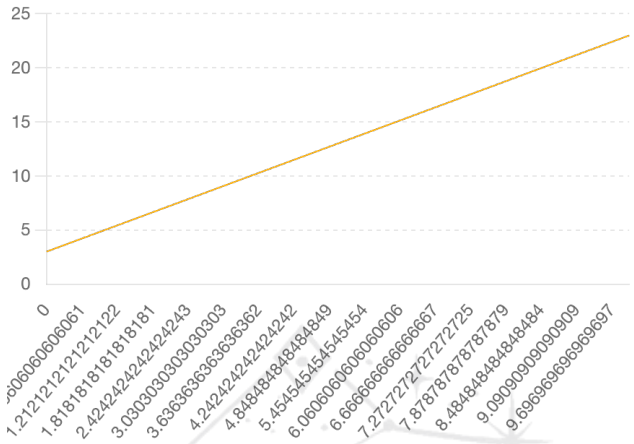
In a Flat / Pro-Rate bonding curve, share price remains constant, minus any share price changes incurred through fees. This may be useful in an environment that benefits from the maximization of entities participating and amount deposited. Above is an example graph of a flat curve represented by the equation:

$y = 5 * y$

Archived copy · cryp2nova.com

The graph depicts a horizontal line, signifying that the value of y remains constant regardless of variations in x. In this context, an individual can consistently redeem the same amount of assets that they initially deposited into the Vault, less any applicable fees.

Linear

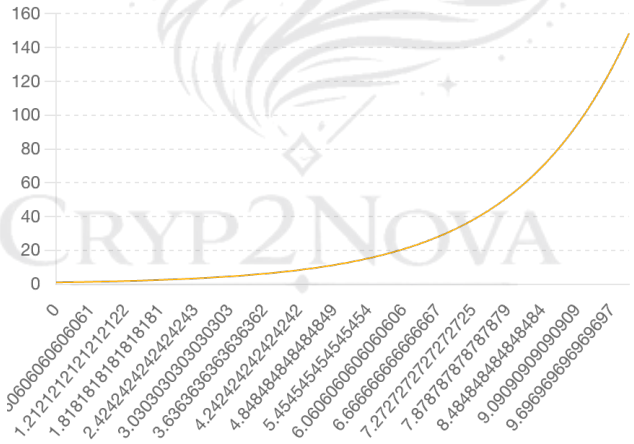


In a linear bonding curve, share price linearly increases. This may be useful in scenarios in which additional signal has diminishing returns, or scenarios in which early signal is more heavily weighted. Provided above is an example graph of a linear curve represented by the equation:

$y = 2 * x + 3$

y. In this context, as the share price increases or decreases along the curve, depositors would be able to redeem more or fewer assets from the vault depending on the current position on the line relative to their deposit points.

Exponential



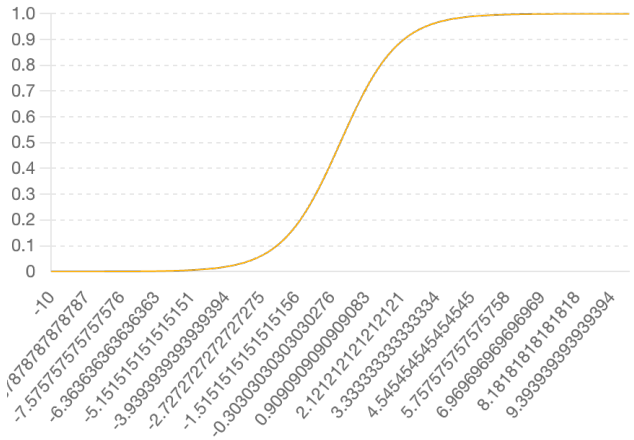
In an exponential bonding curve, share price increases exponentially. This may be useful in the construction of speculative games, providing participants with the potential to generate significant returns. Above is an example graph of an exponential curve represented by the equation:

$y = e^{x/2}$

Sigmoid

Sigmoid curves can provide an interesting environment that encourages participation within a discrete range. This may be useful for a number of purposes, such as when a predetermined amount of collateral is deemed necessary to establish trustworthiness or validity of a claim. Above is a sigmoid curve represented by the equation:

Archived copy · cryp2nova.com



$y = 1/1 + e^{-x}$

A Singular Intuition System

The capability to support arbitrary bonding curves within the Intuition system is essential in preventing fragmentation. If the system were restricted to a single bonding curve, it would inevitably fail to optimize across all use cases. Such limitations would lead to the emergence of multiple, disparate deployments of Intuition, resulting in fragmented data and liquidity—outcomes antithetical to the system's foundational goals.

By allowing developers to customize bonding curves to suit specific requirements, Intuition provides the flexibility necessary to accommodate diverse applications. This adaptability ensures that various use cases can be effectively addressed within a unified framework. Consequently, developers are empowered to design tailored economic models and interactions, thereby enabling the construction of a wide array of applications on top of a singular, cohesive implementation of the Intuition system. This approach preserves the integrity and cohesiveness of the data ecosystem.

Example Fee & Bonding Curve Implementation Value Flows To illustrate the intended behavior, we will examine the value flows within an example implementation utilizing a 'pro-rata' bonding curve for all Vaults. In this model, the Share Price changes solely due to entry and exit fees paid to each vault, ensuring that users cannot lose more than their initial deposit, minus the fees. We will also assume that the initial share price for each Vault is set at 1 (i.e., 1 Asset = 1 Share). All values will be denominated in ETH.

Atom Creation Value Flows Static Atom Cost

Let $C_{atomCreation}$ represent the total amount of static fees for creating an Atom, `atomCost`.

- `protocolCreationFee`: A fixed fee paid to the protocol's multi-signature wallet address., $F_{protocolCreate}$
- `walletInitialDeposit`: A fixed amount deposited on the Atom Vault on behalf of the Atom Wallet, $F_{atomWallet}$
- `minShare`: A minimal number of shares purchased for a neutral address to prevent share price inflation attacks, referred as 'ghost shares', F_{ghost}

The total `atomCost` A_c may be represented as:

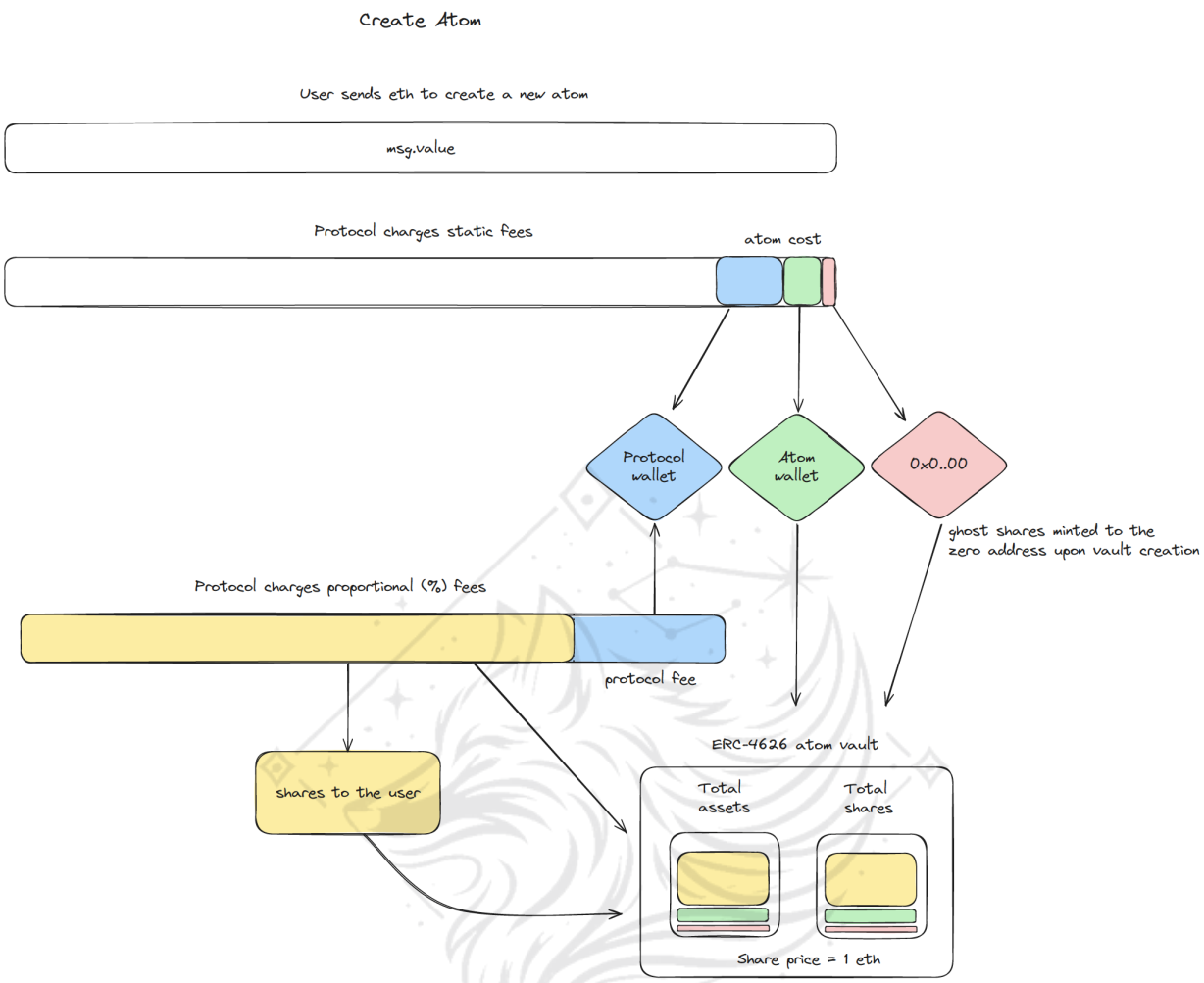
$C_{atomCreation} = F_{protocolCreate} + F_{atomWallet} + F_{ghost}$

Deposit Fees

If `msg.value` exceeds `atomCost`, the remainder is deposited on the `Atom Vault` on behalf of the `msg.sender`, and incurs a `depositFee`, $F_{protocolDeposit}$, paid to the protocol.

- `protocolFeeRate`: The percentage fee applied to the user deposit, to be paid to the protocol, $F_{protocolFeePercent}$

Archived copy · cryp2nova.com



- `userDeposit`: The total amount of assets sent by the user during the create transaction, $A_{userDeposit}$

The additional deposit fee $F_{protocolDeposit}$ is calculated as:

$F_{protocolDeposit} = (A_{user} - C_{atomCreation}) * F_{protocolFeePercent})$

Summary of State After Creation

- `userShares`: Let S_{user} represent the amount of Shares received by the User in the Atom's Vault:
  - $S_{user} = A_{userDeposit} - C_{atomCreation} - F_{protocolDeposit}$
- `userAssets`: Let A_{user} represent the amount of Assets that can be redeemed from the Vault by the User:
  - $A_{user} = S_{user}$, as no `entryFee` is charged during the creation deposit flow; thus, `sharePrice` remains 1:1.
- `totalVaultAssets` = $A_{vaultTotal} = A_{user} + F_{atomWallet} + F_{ghost}$
- `totalVaultShares` = $S_{vaultTotal} = A_{user} + F_{atomWallet} + F_{ghost}$

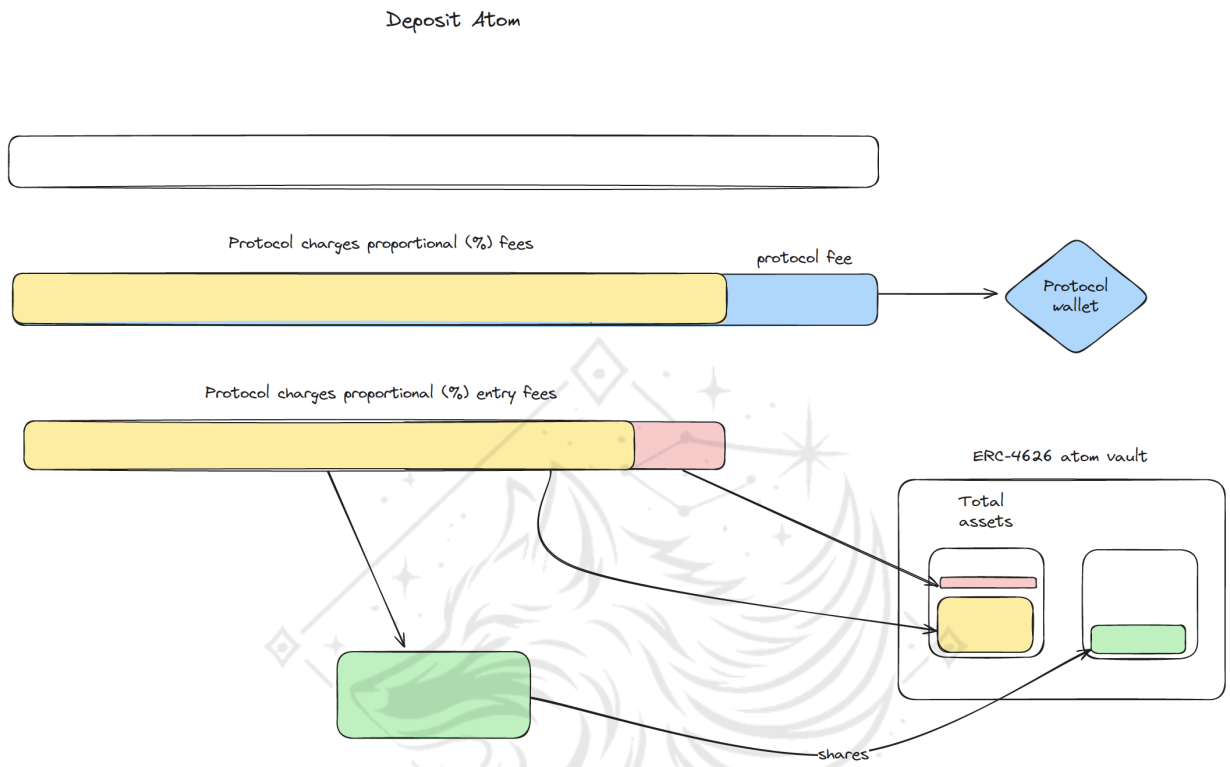
Given that assets will equal shares, the additional allocations are as follows:

- Shares to the Atom wallet address = $F_{atomWallet}$
- Shares to the 0x0 address (lost) = F_{ghost}

Archived copy · cryp2nova.com

- Assets to the Protocol = $F_{protocolCreate} + F_{protocolDeposit}$

Deposit Atom:



Initial Summary of State

- `totalVaultAssetsBefore`: The total Assets in the Vault before the state change introduced by the deposit transaction, $A_{vaultTotalBefore}$
- `totalVaultSharesBefore`: The total outstanding Shares of the Vault before the state change introduced by the deposit transaction, $S_{vaultTotalBefore}$
- `sharePriceBefore`: The amount of Assets (ETH) each share can be redeemed for at the beginning of the transaction, $S_{priceBefore}$
  - $S_{priceBefore} = A_{vaultTotalBefore}/S_{vaultTotalBefore}$

Deposit Fees

Let $F_{atomDeposit}$ represent the total fees paid for depositing on an Atom:

- `msg.value`: The value passed through to the `depositAtom` function, $A_{userDeposit}$
- `protocolFeeRate`: The percentage fee applied to the user deposit, to be paid to the Protocol $F_{protocolFeePercent}$
- `protocolFee`: The fee paid to the protocol, $F_{protocol}$
  - $F_{protocol} = A_{userDeposit} * F_{protocolFeePercent}$
- `entryFeePercent`: The percentage fee applied to the user deposit, that will be paid to the current Vault depositors, $F_{entryFeePercent}$
- `entryFee`: The fee paid to current depositors in the Atom Vault, F_{entry}
  - $F_{entry} = (A_{userDeposit} - F_{protocol}) * F_{entryFeePercent}$

Archived copy · cryp2nova.com

The total Atom Deposit Fee, $F_{atomDeposit}$ may be represented as:

$F_{atomDeposit} = F_{protocol} + F_{entry}$

Summary of State After Deposit

- `userShares`: The amount of Shares received by the User in the Atom's Vault, S_{user}
  - $S_{user} = (A_{userDeposit} - F_{atomDeposit})/S_{priceBefore}$
- `userAssets`: The amount of the Vault's Assets (ETH) that S_{user} can be redeemed for, A_{user}:
  - $A_{user} = A_{userDeposit} - F_{atomDeposit}$
- `totalVaultAssetsAfter`: The total Assets of the Vault after the state change introduced by the deposit transaction, $A_{vaultTotalAfter}$:
  - $A_{vaultTotalAfter} = A_{vaultTotalBefore} + A_{userDeposit} - F_{protocol}$
- `totalVaultSharesAfter`: The total outstanding Shares of the Vault after the state change introduced by the deposit transaction, $S_{vaultTotalAfter}$:
  - $S_{vaultTotalAfter} = S_{vaultTotalBefore} + S_{user}$
- `sharePriceAfter`: The amount of Assets (ETH) each share can be redeemed for after the transaction, $S_{priceBefore}$
  - $S_{priceAfter} = A_{vaultTotalAfter}/S_{vaultTotalAfter}$

With this, the `entryFee` will result in an increase in `sharePrice`, as `totalVaultAssets`, the numerator, will increase more than `totalVaultShares`, the denominator. This allows all current depositors to redeem their Shares from the Vault for an increased `sharePrice`, effectively achieving a distribution of `entryFees` paid to all current shareholders.

Redeem Atom

Initial Summary of State

- `totalVaultAssetsBefore`: The total Assets in the Vault before the state change introduced by the deposit transaction, $A_{vaultTotalBefore}$
- `totalVaultSharesBefore`: The total outstanding Shares of the Vault before the state change introduced by the deposit transaction, $S_{vaultTotalBefore}$
- `sharePriceBefore`: The amount of Assets (ETH) each share can be redeemed for at the beginning of the transaction, $S_{priceBefore}$
  - $S_{priceBefore} = A_{vaultTotalBefore}/S_{vaultTotalBefore}$

Redemption Fees

Let $F_{atomRedeem}$ represent the total fees paid for redeeming Shares of an Atom Vault:

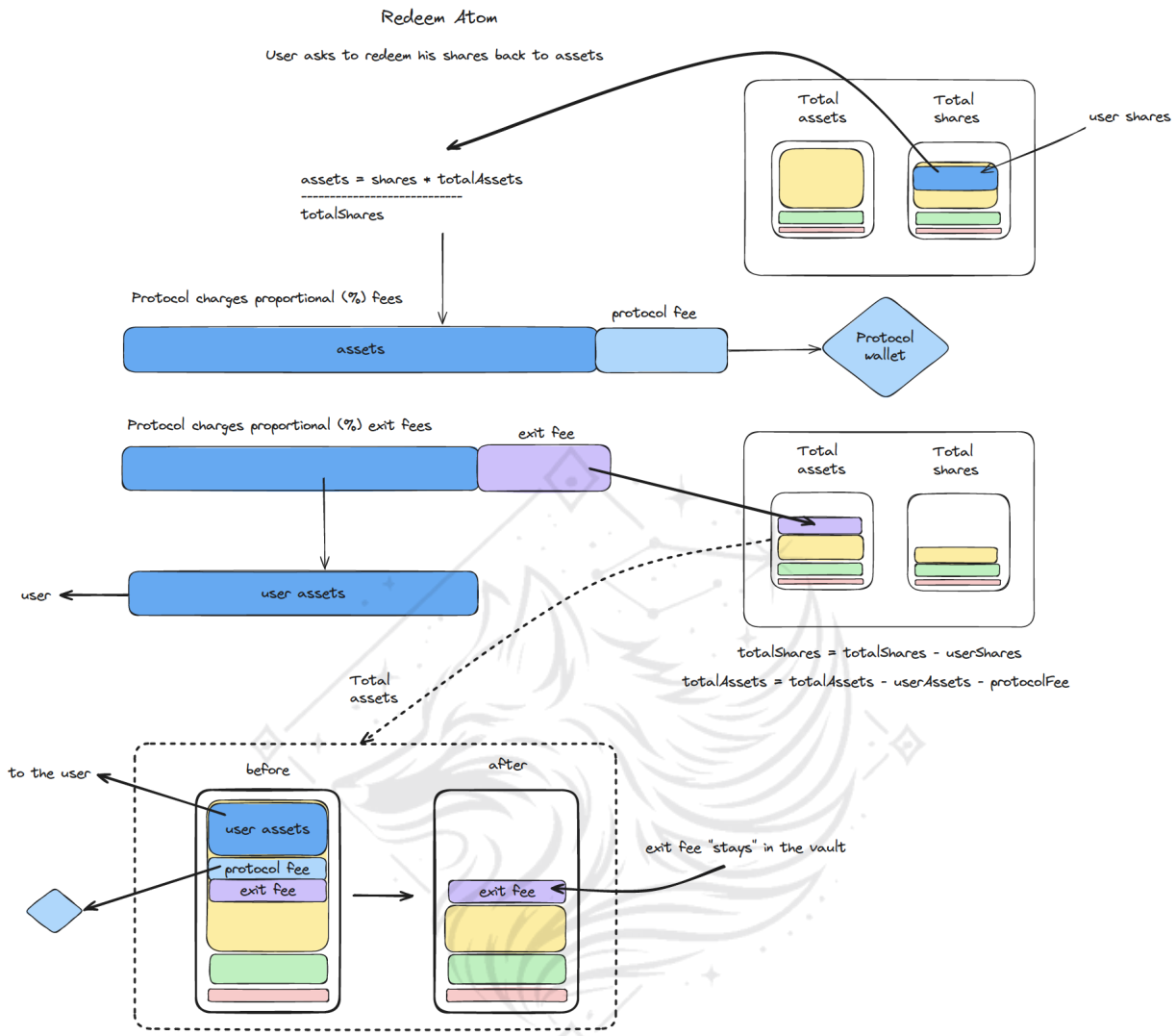
- `redeemAmount`: The amount of Shares to be redeemed, $S_{userRedeem}$
- `protocolFeeRate`: The percentage fee applied to the user redemption, to be paid to the Protocol $F_{protocolFeePercent}$
- `protocolFee`: The fee paid to the protocol, $F_{protocol}$
  - $F_{protocol} = S_{userRedeem} * S_{priceBefore} * F_{protocolFeePercent}$
- `exitFeePercent`: The percentage fee applied to the user redemption, that will be paid to the current Vault depositors, $F_{exitFeePercent}$
- `exitFee`: The fee paid to current depositors in the Atom Vault, F_{exit}
  - $F_{exit} = ((S_{userRedeem} * S_{priceBefore}) - F_{protocol}) * F_{exitFeePercent}$

The total Atom Redemption Fee, $F_{atomRedeem}$ may be represented as:

$F_{atomRedeem} = F_{protocol} + F_{exit}$

Summary of State After Creation

Archived copy · cryp2nova.com



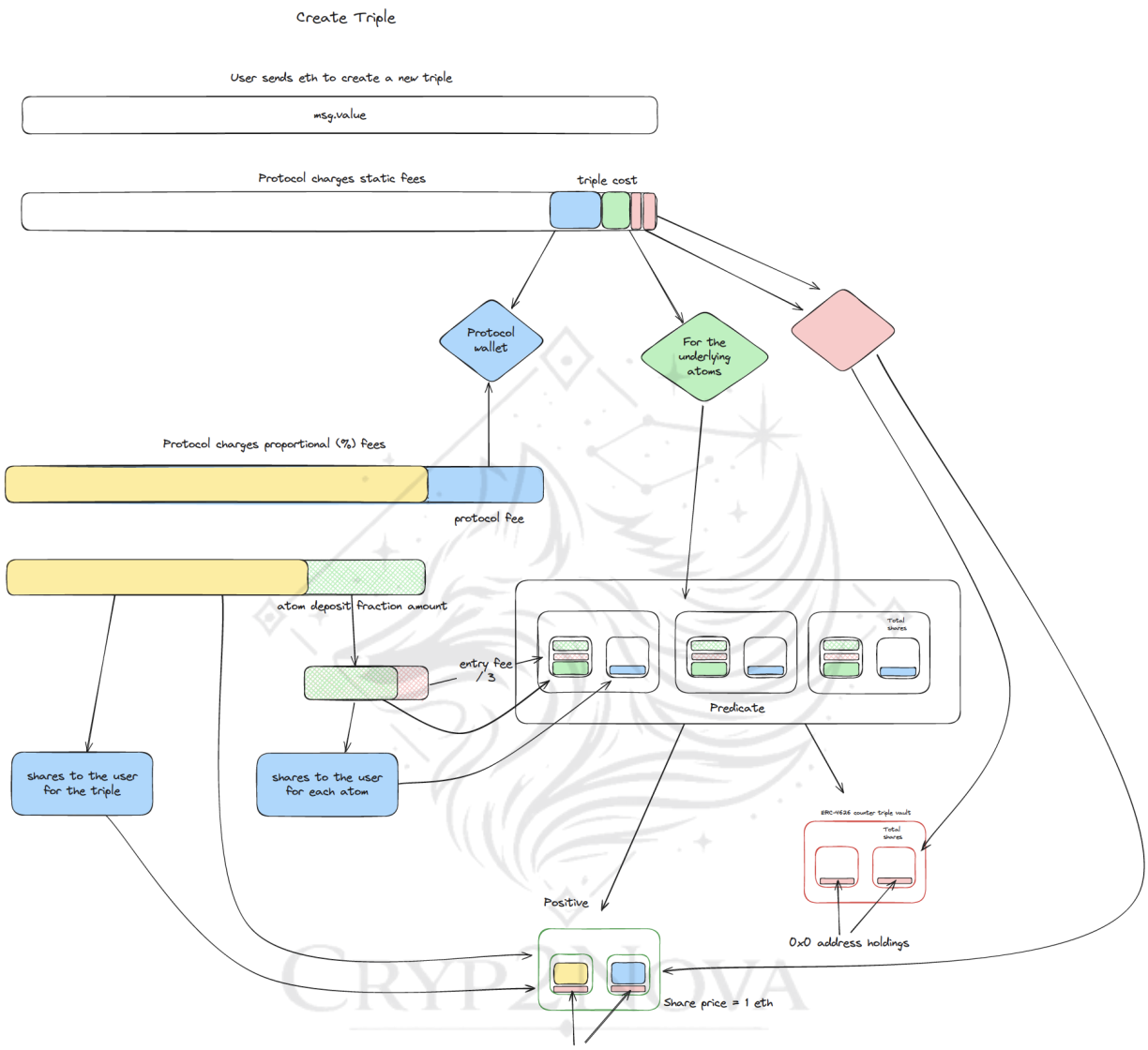
- `userShares`: The amount of Shares owned by the User in the Atom's Vault, S_{user}
  - $S_{user} = S_{userBefore} - S_{userRedeem}$
- `userAssets`: The amount of the Vault's Assets (ETH) received by the user, A_{user}:
  - $A_{user} = (S_{userRedeem} * S_{priceBefore}) - F_{atomRedeem}$
- `totalVaultAssetsAfter`: The total Assets of the Vault after the state change introduced by the redemption transaction, $A_{vaultTotalAfter}$:
  - $A_{vaultTotalAfter} = A_{vaultTotalBefore} - A_{user} - F_{protocol}$
- `totalVaultSharesAfter`: The total outstanding Shares of the Vault after the state change introduced by the redemption transaction, $S_{vaultTotalAfter}$:
  - $S_{vaultTotalAfter} = S_{vaultTotalBefore} - S_{user}$
- `sharePriceAfter`: The amount of Assets (ETH) each share can be redeemed for after the transaction, $S_{priceBefore}$
  - $S_{priceAfter} = A_{vaultTotalAfter}/S_{vaultTotalAfter}$

With this, the `exitFee` will once again result in an increase in `sharePrice`, as `totalVaultAssets`, the numerator, will decrease less than `totalVaultShares`, the denominator. This allows all current depositors

Archived copy · cryp2nova.com

to redeem their Shares from the Vault for an increased `sharePrice`, effectively achieving a distribution of `exitFees` paid to all current shareholders.

Triple Creation Fees



Static Triple Cost

Let $C_{TripleCreation}$ represent the total amount of static fees for creating an Triple, `tripleCost`.

- `protocolCreationFee`: A fixed fee paid to the protocol's multi-signature wallet address, $F_{protocolCreate}$
- `atomFeeOnTripleCreation`: A fixed fee paid to the underlying Atom vaults, $F_{atomFeeOnTripleCreation}$
- `minShare`: A minimal number of shares purchased for a neutral address to prevent share price inflation attacks, referred as 'ghost shares', F_{ghost}. Since each triple has 2 associated Vaults, this amount during Triple creation is $2 * F_{ghost}$.

The total `tripleCost` $C_{tripleCreation}$ may be represented as:

$$C_{tripleCreation} = F_{protocolCreate} + F_{atomFeeOnTripleCreation} + (2 * F_{ghost})$$

Archived copy · cryp2nova.com

Deposit Fees

If `msg.value` exceeds `tripleCost`, the remainder is deposited on the `Triple's Positive Vault` on behalf of the `msg.sender`. This process incurs an additional deposit fees paid to the Protocol, $F_{protocolDeposit}$.

- `protocolFeeRate`: The percentage fee applied to the user deposit, $F_{protocolFeePercent}$
- `userDeposit`: The total amount of assets sent by the user during the create transaction., $A_{userDeposit}$

The additional deposit fee $F_{protocolDeposit}$ is calculated as:

$F_{protocolDeposit} = (A_{userDeposit} - C_{TripleCreation}) * F_{protocolFeePercent})$

As per the default Triple deposit flow, outlined in the subsequent section, a portion of this deposit amount is also deposited into each of the Triple's underlying Atoms, `atomDepositFraction`. Let `atomDepositFraction` be represented by $F_{tripleAtomDeposit}$.

$F_{tripleAtomDeposit} = ((A_{user} - C_{tripleCreation}) - F_{protocolDeposit}) * F_{tripleAtomDepositPercent}$, where $F_{tripleAtomDepositPercent}$ is the percent of the deposit routed to the Atom Vaults.

Summary of State After Creation

Triple State

- `userTripleShares`: The amount of Shares received by the User in the Triple's Positive Vault, $S_{userTriple}$
  - $S_{userTriple} = A_{userDeposit} - C_{tripleCreation} - F_{protocolDeposit}$
- `userTripleAssets`: The amount of Assets that can be redeemed from the Triple's Positive Vault by the User, $A_{userTriple}$
  - $A_{userTriple} = S_{userTriple}$, as no `entryFee` is charged during the creation deposit flow; thus, `sharePrice` remains 1:1.
- `totalVaultAssets` = $A_{vaultTotal} = A_{userTriple} + F_{ghost}$
- `totalVaultShares` = $S_{vaultTotal} = A_{userTriple} + F_{ghost}$

Atom State

- `userAtomShares`: Let S_{user} represent the amount of Shares received by the User in each respective Atom Vault:
  - $S_{user} = (F_{tripleAtomDeposit}/3)/S_{priceBefore}) - ((F_{tripleAtomDeposit}/3)/S_{priceBefore}) * F_{entry})$, where $S_{priceBefore}$ is the `sharePrice` of each respective Atom Vault, and F_{entry} is the `entryFee` of each Atom Vault.
- `userAtomAssets`: Let A_{user} represent the amount of Assets that can be redeemed from each respective Atom Vault by the User:
  - $A_{user} = S_{user}$ * $S_{priceAfter}$, where $S_{priceAfter}$ is the Share Price of each Atom Vault after the transaction. This can be calculated in the same way as in the 'Atom Deposit' section above, as this is a normal Atom Deposit event.

Protocol State

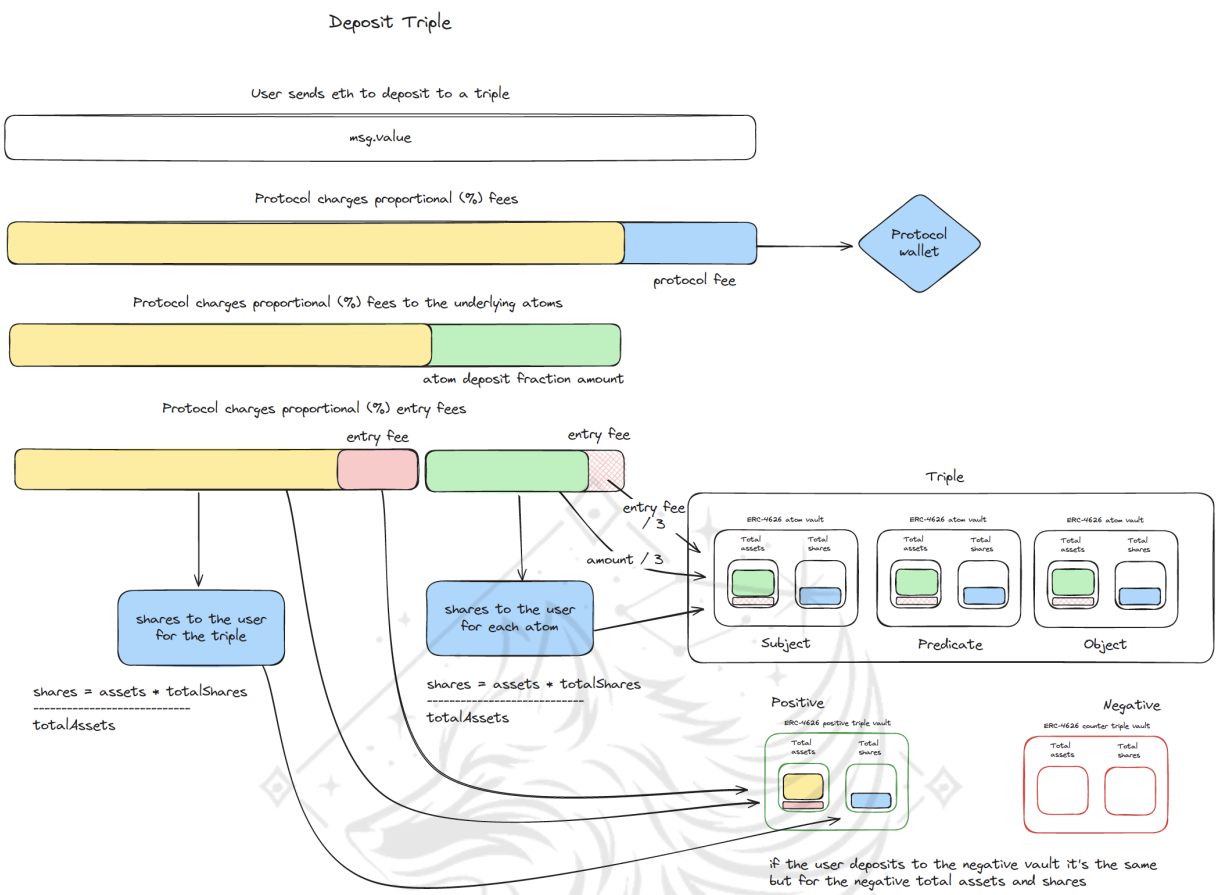
- Assets to the Protocol = $F_{protocolCreate} + F_{protocolDeposit}$

Deposit Triple

Initial Summary of State

- `totalVaultAssetsBefore`: The total Assets in the Vault before the state change introduced by the deposit transaction, $A_{vaultTotalBefore}$
- `totalVaultSharesBefore`: The total outstanding Shares of the Vault before the state change introduced by the deposit transaction, $S_{vaultTotalBefore}$
- `sharePriceBefore`: The amount of Assets (ETH) each share can be redeemed for at the beginning of the transaction, $S_{priceBefore}$

Archived copy · cryp2nova.com



- $S_{priceBefore} = A_{vaultTotalBefore} / S_{vaultTotalBefore}$

Deposit Fees

Let $F_{TripleDeposit}$ represent the total fees paid for depositing on an Triple:

- `msg.value`: The value passed through to the `depositTriple` function, $A_{userDeposit}$
- `protocolFeeRate`: The percentage fee applied to the user deposit, to be paid to the Protocol $F_{protocolFeePercent}$
- `protocolFee`: The fee paid to the protocol, $F_{protocol}$
  - $F_{protocol} = A_{userDeposit} * F_{protocolFeePercent}$
- `entryFeePercent`: The percentage fee applied to the user deposit, that will be paid to the current Vault depositors, $F_{entryFeePercent}$
- `atomDepositFraction`: The amount of value that will be routed through the Atom Deposit flow for each of the Triple's respective Atom Vaults, $F_{tripleAtomDeposit}$
  - $F_{tripleAtomDeposit} = (A_{userDeposit} - F_{protocol}) * F_{tripleAtomDepositPercent}$
- `entryFee`: The fee paid to current depositors in the Triple Vault, F_{entry}
  - $F_{entry} = (A_{userDeposit} - F_{tripleAtomDeposit} - F_{protocol}) * F_{entryFeePercent}$

The total Triple Deposit Fee, $F_{atomDeposit}$ may be represented as:

$F_{atomDeposit} = F_{protocol} + F_{entry}$

Triple State

Archived copy · cryp2nova.com

- `userTripleShares`: The amount of Shares received by the User in the Triple's Vault, S_{user}
  - $S_{user} = (A_{userDeposit} - F_{atomDeposit} - F_{tripleAtomDeposit})/S_{priceBefore}$
- `userTripleAssets`: The amount of the Vault's Assets (ETH) that S_{user} can be redeemed for, A_{user}:
  - $A_{user} = A_{userDeposit} - F_{atomDeposit} - F_{tripleAtomDeposit}$
- `totalVaultAssetsAfter`: The total Assets of the Vault after the state change introduced by the deposit transaction, $A_{vaultTotalAfter}$:
  - $A_{vaultTotalAfter} = A_{vaultTotalBefore} + A_{userDeposit} - F_{protocol}$
- `totalVaultSharesAfter`: The total outstanding Shares of the Vault after the state change introduced by the deposit transaction, $S_{vaultTotalAfter}$:
  - $S_{vaultTotalAfter} = S_{vaultTotalBefore} + S_{user}$
- `sharePriceAfter`: The amount of Assets (ETH) each share can be redeemed for after the transaction, $S_{priceBefore}$
  - $S_{priceAfter} = A_{vaultTotalAfter}/S_{vaultTotalAfter}$

Atom State

- `userAtomShares`: Let S_{user} represent the amount of Shares received by the User in each respective Atom Vault:
  - $S_{user} = (F_{tripleAtomDeposit}/3)/S_{priceBefore}) - ((F_{tripleAtomDeposit}/3)/S_{priceBefore}) * F_{entry})$, where $S_{priceBefore}$ is the `sharePrice` of each respective Atom Vault, and F_{entry} is the `entryFee` of each Atom Vault.
- `userAtomAssets`: Let A_{user} represent the amount of Assets that can be redeemed from each respective Atom Vault by the User:
  - $A_{user} = S_{user} * S_{priceAfter}$, where $S_{priceAfter}$ is the Share Price of each Atom Vault after the transaction. This can be calculated in the same way as in the 'Atom Deposit' section above, as this is a normal Atom Deposit event.

Redeem Triple

The mechanics of the "Redeem Triple" function operate in exactly the same manner as the "Redeem Atom" function. When a user redeems from a Triple Vault, they are not required to redeem shares of the underlying Atoms that constitute the Triple. This contrasts with the "Deposit Triple" event, where the user must deposit into each respective Atom, introducing a variance between the mechanics of Triple Deposits and Atom Deposits.

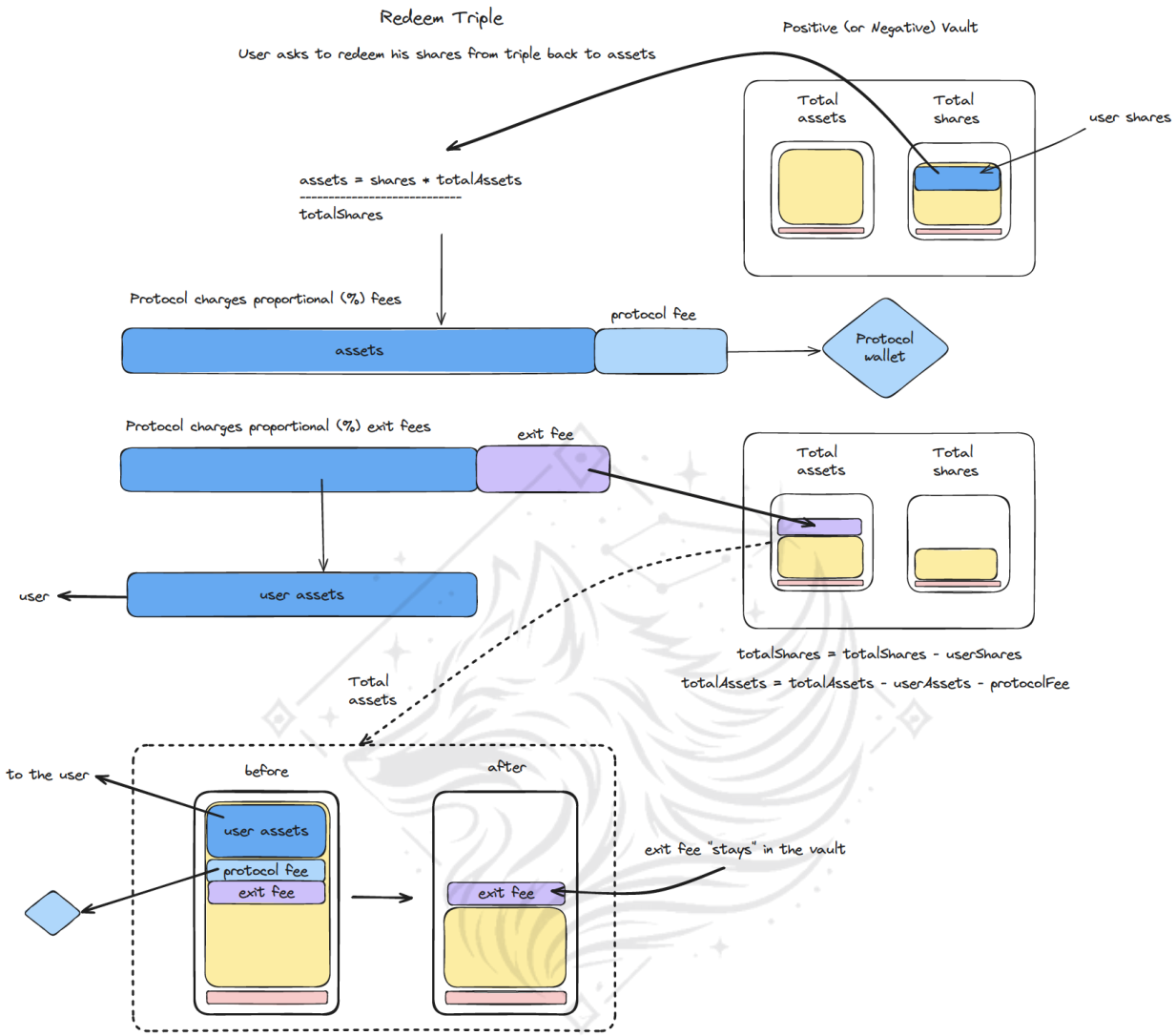
8.5.6 State Interpretation

Having examined the composition of the Intuition state and understood the multi-dimensional graph it generates, we can now explore methods for interpreting this state. The Intuition protocol is designed to maintain a fundamentally neutral stance on the interpretation of its state, refraining from expressing any opinions on what is true or false, or right or wrong. This neutrality allows for a broad spectrum of interpretations to be built upon the foundational data. The aim is to decouple not only identities and data from the application layer but also the algorithms that process and interpret this data. By providing a neutral base, Intuition empowers users and developers to create their own lenses for viewing and understanding the data.

With this unbiased foundation, anyone can permissionlessly create arbitrary interpretations on top of the Intuition protocol. This capability is essential for fostering an ecosystem where diverse algorithms and interpretations can filter, weight, and distill data in various ways. Users can select the interpretations and algorithms that best meet their specific needs, promoting a dynamic and customizable data experience. This flexibility ensures that the system can adapt to a wide range of use cases and perspectives.

This approach addresses a significant issue with many current platforms, where users are confined to a single, often biased, interpretation of data. For instance, platforms like Twitter enforce a single algorithmic perspective, limiting users' ability to see data through different lenses. Intuition's strategy of decoupling algorithms from the platform mitigates this issue, enabling users to toggle between various algorithms and perspectives. This flexibility is crucial for fostering a richer, more inclusive understanding of data, where multiple viewpoints can coexist and be explored.

Archived copy · cryp2nova.com



CRYP2NOVA

Classifications of Interpretation

As previously outlined, interpretation can generally be categorized into three types: literal interpretations, algorithms, and reality tunnels. Given Intuition's unopinionated stance, it does not dictate how data should be sorted or filtered. Nonetheless, these aspects are critical and must be developed. Therefore, Intuition can provide the guardrails and incentives for the contribution of new interpretations, algorithms, and reality tunnels.

Atoms and Triples can be utilized for this purpose, as anything can be represented as an Atom or Triple. With Intuition, TCRs (Token Curated Registries) of interpretations, algorithms, and reality tunnels can be curated, allowing developers and users to easily discover those that might be most suitable for their specific context or use case.

Literal Interpretations

Consider what an Interpretation Registry for the Intuition state might look like when implemented on Intuition. Suppose Organization X uses a 'literal interpretation' to enable a 'follow' functionality in their application, expressed as `{[I] [am following] [User]}`, where the Subject `[I]` and the Predicate `[am following]` remain constant across all Triples, with only the Object changing based on the user being

Archived copy · cryp2nova.com

followed. Additionally, assume that Organization X interprets users with a positive balance in the Positive Vault of the respective Triple as followers of the Object.

While this interpretation serves the purposes of Organization X, they might opt to create another Triple referencing this structure, designating it as a literal interpretation. For example, this could be represented as `{[Organization X Official Interpretation List] [itemListElement] {[I] [am following] [Object]}}`. Utilizing this standardized Triple structure, Organization X could efficiently develop a dashboard displaying all Objects of Triples staked on by Organization X, with the Subject `[Organization X Official Interpretation List]` and Predicate `[itemListElement]`. This would generate a comprehensive list of all officially recognized interpretations by Organization X.

Organization X is incentivized to establish and make their Interpretation discoverable because adoption by others could result in economic rewards through fee revenue. It is presumed that Organization X would hold equity in this data structure, accrued through their usage and adoption of the data structure in question.

To further enhance the utility of this data, Organization X could create additional Triples, such as:

- `{[Organization X Official Interpretation List] [itemListElement] {[I] [am following] [Object]}}`, which could be used to populate an official Intuition Interpretation Registry of Registries
- `{[I] [am following] [Object]} [hasType] [Follow Interpretation]}`, which could be used to populate a list of all Follow Interpretations

Algorithms and Reality Tunnels

The principles applied to literal interpretations can similarly be extended to algorithms and reality tunnels within the Intuition ecosystem. By decoupling the algorithms from the platform, users can create, share, and adopt various algorithmic interpretations to suit their specific needs. This flexibility ensures that users are not restricted to a singular, potentially biased viewpoint but can explore data through multiple, diverse lenses.

For example, consider an algorithm designed by Organization Y to rank content based on user engagement metrics. This algorithm could be represented as a Triple:

`{[Organization Y Algorithm] [ranks] [Content]}`

Users who prefer content ranked by engagement can adopt this algorithm, thereby tailoring their data experience to their preferences. Organization Y can further enhance this by registering their algorithm in the Intuition registry, making it discoverable and accessible to a broader audience. The same structure applies to reality tunnels, which are more comprehensive frameworks that shape users' overall data experiences. A reality tunnel could include a combination of algorithms and interpretations, offering a unique perspective on the data.

Key Variables in State Interpretation In developing literal interpretations, algorithms, and reality tunnels, numerous data aspects are crucial when interpreting the state of the Intuition system. Below is a list of some criteria that may be valuable for developing data filtering techniques:

1. **Amount of Value Deposited on Each Atom**
2. **Amount of Value Deposited on Triples Referencing Each Atom**
3. **Amount of Value Deposited by the Atom into the System**
4. **Self-Claims** ***(Atoms self-attesting to something)***
5. **Temporal Dynamics,** such as the duration and recency of actions taken.
6. **Contextual Reputation of Atoms**
7. **Endorsement Dynamics,** such as mutual endorsements, endorsements within cliques, etc.
8. **Contribution Quality,** such as the truthfulness of historical claims made by an Atom
9. **Interaction Frequency**
10. **Cross-Platform Reputation,** involving reputation of an entity represented by an Atom across platforms.
11. **Economic Behavior,** which may influence the Signal an Atom generates.

Archived copy · cryp2nova.com

12. **Sentiment Analysis,** such as whether or not an Atom is generally positive or negative in its expression.

This limited subset of variables illustrates the inherent complexity and multidimensionality of the Intuition system. It is impractical to assign a single 'score' to entities or to definitively determine what is true or false, right or wrong. Instead, trust should be considered relative and context-dependent, based on the observer's perspective, similar to how trust is established in natural human interactions. This approach can be facilitated by 'lenses' that filter data, which can be permissionlessly developed and equipped but should never be locked into a singular mode of imposed groupthink.

Example Algorithm: Confidence Score Based on Stake Over Time

To demonstrate an example rudimentary Intuition-specifc algorithm, consider a confidence score based on stake over time. Positive Stake over time would result in a Positive Weight, while Negative Stake over time would result in a Negative Weight. The difference between these two weights could be used to calculate a single 'Weight', though this would merely be a metric that parties could observe to better understand the underlying record of activities.

Let P be the amount of positive stake and N be the amount of negative stake. The variance C between positive and negative stakes at any given point in time is defined as:

$C = P - N$

For a given interval of time, the total variance W_c is the sum of all C values within that interval:

$W_c = \sum_{i=1}^{n} C_i = \sum_{i=1}^{n} (P_i - N_i)$

Where i can represent the block number or any other discrete time interval.

This example illustrates the potential that exists at the higher levels of the technological stack. While the Intuition protocol itself does not compute, enforce, or depend on these types of interpretations, it allows for anyone to permissionlessly analyze its state to extract meaningful insights or to develop additional codified logic. In this context, the temporal dimension of this basic algorithm is particularly noteworthy. Locking up economic bandwidth for extended periods can serve as a robust indicator of a user's confidence or belief in a particular entity. This characteristic could be leveraged for various incentivization schemes. For instance, envision a protocol that rewards users based on their sustained positive sentiment towards the protocol over time.

Example Algorithm: EigenTrust

To explore a slightly more complex model, let us consider the EigenTrust Algorithm. The EigenTrust algorithm is a reputation management system that uses a global trust value for each participant in a peer-to-peer network. It works by assigning each peer a trust score based on their history of interactions. The algorithm iteratively computes these trust values based on local trust scores and propagates them through the network.

Here is the basic formula and steps involved:

1. **Local Trust Calculation**: Each peer i computes a local trust value c_{ij} for each other peer j they have interacted with. This is based on the number of satisfactory interactions s_{ij} minus the number of unsatisfactory interactions d_{ij}
   $c_{ij} = s_{ij} - d_{ij} / \sum_k (s_{ik} - d_{ik})$
2. **Normalization**: The local trust values are normalized to ensure they sum to 1 for each peer i:
   $\sum_j c_{ij} = 1$
3. **Global Trust Calculation**: The global trust value t_j for each peer j is computed by iteratively aggregating the local trust values. Starting with an initial trust vector t^0, typically with equal trust for all peers, the trust vector is updated iteratively:
   $t^{k+1} = C^T t^k$
   Here, C is the matrix of normalized local trust values, t^k is the trust vector at iteration k, and t^{k+1} is the trust vector at iteration $k+1$. The iterations continue until t converges, i.e., changes between iterations are below a certain threshold.
4. **Convergence**: The algorithm converges to the stationary distribution of the trust values, representing the global trust scores of the peers.

Archived copy · cryp2nova.com

With this, we have just two of infinite possible interpretations of the state of the Intuition system. With the development of new interpretations comes the unlocking of new potential use cases. As users and developers create various algorithms and reality tunnels, the versatility and applicability of the Intuition protocol expand, leading to a multitude of innovative applications.

9 Use Cases, Examples, & Implications

9.1 Web3 Use Cases & Examples

9.1.1 Transaction Security & Web3 Navigability

The current landscape of Web3 interactions through wallets like MetaMask often presents users with a complex and opaque interface. When interacting with smart contracts or sending transactions, users typically see non-human-readable data strings, transaction hashes, and cryptic addresses, offering little context or insight into the nature and safety of their actions. This lack of clarity can lead to uncertainty and even security risks, as users are unable to easily assess the trustworthiness of the entities they are interacting with.

With Intuition data integrated into wallets like MetaMask, users can see comprehensive and meaningful information about the contracts and addresses they interact with. For instance, when a user is about to engage with a smart contract, the wallet can display data about who has audited the contract and their corresponding reputation scores. This may help provide trust around contract security and the fact that the contract being interacted with is the *correct* contract.

Integrating Intuition data into Web3 wallets also addresses the critical issue of scams and fraudulent activities. Users can see if a particular address has been flagged as a scammer by the community, based on collective attestations. For example, if numerous users have reported a specific address as a phishing scam, this warning can be prominently displayed within the wallet interface, alerting the user to proceed with caution or avoid the interaction altogether.

The open and permissionless nature of Intuition's data lake ensures that this information is continuously updated and verified by the community, enhancing its reliability. By leveraging the collective intelligence and vigilance of the decentralized ecosystem, Web3 wallets can provide a more secure and trustworthy environment for users.

Beyond security, the integration of Intuition data can enrich the user experience by providing semantic context to transactions. Users could see labels and descriptions for tokens, contracts, and addresses based on community-generated data. For example, a token address could be accompanied by a description of the token's purpose, the project behind it, and user reviews or ratings, without reliance on an intermediary such as Coingecko. This semantic enrichment makes the data more accessible and understandable, even for users who may not have deep technical knowledge.

Furthermore, this enriched context can be personalized based on the user's trust graph. By leveraging the trust relationships established within Intuition, wallets can prioritize information and recommendations from sources that the user personally trusts, creating a more tailored and relevant experience.

9.1.2 Developer Tooling Discoverability

The rapid pace of innovation in the Web3 and blockchain space has led to a proliferation of developer tools, frameworks, and libraries. While this wealth of resources is a boon for developers, it also presents a significant challenge: keeping track of the latest and most effective tools is increasingly difficult. The current ecosystem suffers from fragmentation, with many valuable tools going unnoticed or underutilized, leading to duplicated efforts and inefficiencies. Intuition offers a solution by leveraging the power of crowdsourced knowledge to create comprehensive, dynamic, and easily navigable lists of developer tools.

With new tools and frameworks being released frequently, developers face the daunting task of staying updated and identifying the best resources for their needs. The decentralized nature of the Web3 space further complicates this, as information is scattered across various platforms and repositories. This fragmentation not only hampers productivity but also leads to the unintentional duplication of work, as developers may unknowingly create tools that already exist.

Intuition tackles this problem by providing a platform for the community to collectively categorize, review, and endorse developer tools. By aggregating and organizing data through user contributions, Intuition en-

Archived copy · cryp2nova.com

sures that valuable resources are easily discoverable, reducing the time and effort developers spend searching for the right tools.

Intuition enables users to tag and categorize developer tools based on their functionality, use cases, and other relevant criteria. When a developer organizes their own toolkit—by tagging a new library or framework as "smart contract development" or "Ethereum scaling solution"—this information is shared with the entire Intuition ecosystem. This crowdsourced approach ensures that the collective knowledge and experience of the developer community are harnessed to create a comprehensive and up-to-date repository of tools.

For instance, a developer might discover a new tool that simplifies the process of deploying smart contracts. By tagging and categorizing this tool within Intuition, they not only organize their own resources but also make this tool discoverable to others who might benefit from it. This collaborative effort helps prevent the duplication of work and encourages the adoption of the best available tools.

Intuition's decentralized and permissionless data lake allows for the creation of a dynamic and interconnected knowledge base. As more developers contribute to the platform, the repository of developer tools grows richer and more nuanced. Each tool's entry can include detailed descriptions, user reviews, and endorsements from trusted community members, providing a holistic view of its capabilities and reliability.

This interconnected knowledge base enables developers to quickly find the tools they need, understand their use cases, and assess their quality based on community feedback. The ability to access this wealth of information in one place significantly enhances the efficiency of the development process.

Leveraging Intuition's personalized trust graphs, developers can receive tailored recommendations based on their specific needs and preferences. By overlaying their trust graph onto the list of developer tools, they can prioritize recommendations and endorsements from individuals and organizations they trust. This personalized approach helps developers navigate the vast array of tools and focus on those most relevant to their projects.

For example, if a developer trusts the recommendations of a well-known blockchain development team, they can see which tools this team endorses and uses. This not only streamlines the discovery process but also provides an additional layer of confidence in the quality and reliability of the tools selected.

9.1.3 Delegate Reputation

In the Web3 ecosystem, decentralized governance is highly prized, and the decision to delegate tokens or voting power plays a critical role in the success of decentralized projects. However, the current processes for vetting and selecting DAO (Decentralized Autonomous Organization) delegates are deeply flawed. Despite the value placed on pseudonymity, control over multi-billion-dollar protocols is often handed to individuals who haven't undergone proper vetting and may lack the necessary expertise. The typical vetting process is superficial, relying on factors like usernames, profile pictures, or brief bios, which fall far short of what's needed. Users are expected to conduct their own thorough due diligence, which is impractical in a decentralized environment where individual stakes are usually too small to justify the effort. Even when due diligence is performed, the data available is often unreliable, with falsified credentials being a common issue.

Intuition offers a solution by providing tools that enable the verification of key information, such as who made specific claims about what, and at what time—for example, a university verifying that an individual graduated with a specific degree, or an employer confirming that someone worked for them. Additionally, Intuition incentivizes community members to share more data points, helping to build a more comprehensive picture of an individual's reputation within the ecosystem.

The semantic structuring of this data allows users to easily navigate and filter through trust networks, or "trust circles," within specific contexts. This means that users can view data, sentiment, and opinions filtered through people they trust within relevant fields. For instance, users could identify which experts in a particular area endorse a specific delegate or staking operator. Contextual reputation is key here—knowing that an entity has a high general reputation is less valuable than understanding their reputation within the specific context of their role. For example, a delegate's expertise in managing hardware and software operations is far more relevant to their role in a DAO than their reputation in unrelated areas like sports or entertainment.

Furthermore, this system incentivizes delegates to act in the best interests of the protocol, as their actions directly impact their reputation within the Intuition system. A transparent, aggregated trust score, derived from the collective input of the Web3 community, provides a more accurate and holistic view of their capabil-

Archived copy · cryp2nova.com

ities and track record. This reputation score can then be used as a credential, unlocking new opportunities and offering tangible benefits that may have previously been out of reach.

9.1.4 Credit Scores

In the traditional financial system, credit scores are pivotal for accessing financial services, yet they often rely on limited, centralized data that doesn't fully capture an individual's financial behavior or potential. This approach can exclude those without established credit histories, such as young adults or individuals in underserved regions, limiting their access to financial opportunities.

Intuition can revolutionize credit scoring by leveraging decentralized attestations and community-driven reputation systems. Here, creditworthiness is determined not just by traditional financial data but also by a comprehensive array of attestations—both objective and subjective. These attestations provide deeper insights into an individual's financial behavior. For example, when someone borrows money, the lender can attest to their reliability, timeliness in repayment, and overall trustworthiness. These attestations, whether formal statements or subjective opinions, are recorded, timestamped, and integrated into the borrower's decentralized credit profile, creating a nuanced and dynamic credit score.

One of the key innovations of Intuition is the ability to leverage this reputation as collateral. If Intuition is widely adopted and people invest significant time and resources into building their reputations, these reputations themselves acquire tangible value. A strong reputation within the Intuition system could become a valuable asset that can be used to secure loans. Since the reputation is built on a foundation of community-validated attestations, any attempt to undermine it would need to outweigh the value of that reputation. This makes malicious attacks costly and impractical, further reinforcing the trust and reliability of the system.

Imagine a scenario where, based on your Intuition reputation, you could borrow money with the assurance that the loan amount is less than the value of your reputation. The system inherently discourages defaulting, as the cost to one's reputation—and the associated loss of future opportunities—would far exceed the benefit of a short-term gain. This creates a powerful incentive for individuals to maintain and protect their reputations, knowing that their standing within the community holds real, tangible value.

By focusing on decentralized attestations, subjective claims, and the intrinsic value of reputation, Intuition not only democratizes access to credit but also fosters a more secure and fair financial ecosystem. This system empowers individuals to build, leverage, and protect their financial identity, offering a credit score that truly reflects their behavior, trustworthiness, and the confidence others have in them.

9.2 Web2 Use Cases & Examples

9.2.1 Media & News

In the current landscape of media, manipulation and misinformation are pervasive issues that undermine the integrity of public discourse. The rapid spread of misinformation and disinformation and the strategic use of propaganda tactics can significantly distort public perception and decision-making. Intuition provides a framework to mitigate these challenges by enhancing transparency, accountability, and trustworthiness in information dissemination.

One of the key features of Intuition is its ability to trace the provenance of data. Intuition ensures that the origin and history of information are transparent and verifiable. This transparency allows users to trace the source of information to its origin, determining its credibility and authenticity. By examining the history of data and users, individuals can evaluate the consistency and reliability of the sources over time. Transparency in data provenance helps identify alterations or misrepresentations, making it more difficult for malicious actors to manipulate information without detection.

Additionally, Intuition's opt-in state interpretation mechanisms, such as the ability to toggle between Reality Tunnels, ensure that no one is locked into a single, manipulative echo chamber. This feature helps users discern trustworthy information from manipulative or false narratives, providing a more balanced perspective on the information they encounter.

Intuition also enables a community-driven approach to fact-checking. Similar to 'community notes' on platforms like Twitter, but applicable to the entire internet, Intuition leverages the collective intelligence and expertise of its users. This community-driven model allows for real-time policing to ensure higher data quality and accuracy.

Archived copy · cryp2nova.com

Consider the context of a major political election. In such a scenario, misinformation and propaganda can significantly influence voter behavior. Intuition can help mitigate these effects by providing a transparent and accountable information ecosystem. In Intuition, people can express their thoughts and opinions freely, without risk of censorship, bias, or manipulation. Political statements and campaign promises can be recorded on Intuition, with their origins and subsequent modifications transparently documented. Voters can verify the authenticity and consistency of these statements. News articles and reports can be evaluated based on their source reputation and content quality, allowing voters to access information from high-reputation sources and reducing the risk of being misled by biased or false reporting.

By providing tools for verifying the authenticity of information, Intuition empowers individuals to make more informed decisions. Ensuring that voters have access to accurate and reliable information strengthens the democratic process and protects it from manipulation. Transparent and accountable information dissemination fosters a healthier public discourse, where ideas can be debated based on their merits rather than misinformation. By reducing the prevalence of manipulation, Intuition can help restore trust in our media, building a more informed and engaged society.

9.2.2 Reviews

The landscape of reviews in Web2 is fundamentally broken.

Identity fragmentation makes it difficult to reconcile reviews across platforms. As new platforms emerge, they compete for data, leading to further fragmentation. Although building aggregators is possible, Web2 companies often restrict access to their data, charge exorbitant fees for API usage, or eliminate access entirely, as their data is their moat.

Data fragmentation exacerbates the problem. Users frequently express themselves through unstructured text in closed environments, such as group chats and verbal conversations. Without a suitable platform that ensures this data reaches the intended recipients, data remains fragmented and disconnected.

A significant issue is the lack of incentives for users to leave reviews on these platforms meant to aggregate communal sentiment. These incentives can be categorized into four main areas:

- **Economic Incentives**: Currently, platforms like Amazon typically do not offer financial rewards for consumers to leave reviews.
- **Reputational Incentives**: There is no mechanism for users to build and benefit from a reputation as reviewers within or outside most platforms.
- **Educational Incentives**: Users have no certainty that their reviews will be seen by people they care about, discouraging them from investing time and effort.
- **Functional Incentives**: Reviewing products does not provide any practical utility to the user, aside from maybe occasionally serving as an outlet for frustrations.

Due to these limitations, most users do not contribute reviews, even though most people relies on these reviews to make daily decisions. The absence of a better alternative forces reliance on fragmented and unreliable data to discern who or what to trust online.

Intuition introduces a paradigm where every ***thing*** - including you, your network, and the things you are reviewing - has a canonical decentralized identifier, making it universally referenceable across the web. Imagine leaving a review on a product in an Intuition-enabled app, and having it seamlessly propagate across all platforms that display reviews. Furthermore, imagine carrying your social and trust graphs, along with all your data, wherever you go. There would be no need to rejoin communities, rebuild follower lists, or repeatedly create profiles and set preferences. For instance, when shopping for supplements on Amazon, you could see recommendations from experts in your global 'supplements trust graph'. When searching for AI podcasts on Spotify, you would see recommendations from trusted individuals in the AI field.

Envision being compensated for sharing useful information. Liking a YouTube video could earn you money for each subsequent like it receives. You could build a reputation as a trusted reviewer of content or products. Your social graph or followers could always see your opinions if they wished—whether you liked a YouTube video, which supplements your trusted expert recommends, or which influencers in Web3 to follow.

Furthermore, if users could take their reputation as a reviewer and use it elsewhere, such as in the process of securing an undercollateralized loan in decentralized finance (DeFi), the incentive to build and maintain a

Archived copy · cryp2nova.com

good reputation would be much stronger. The ability to leverage their reviewer reputation in other contexts would enhance the value of leaving reviews, fostering a more interactive and community-driven environment.

By allowing for the capture of many-to-one, non-deterministic attestations and incentivizing people economically to participate in this process, Intuition provides a powerful tool for enhancing the value and impact of reviews across all platforms. This system not only improves the reliability and trustworthiness of reviews but also creates a more interconnected and motivated community of reviewers, ultimately leading to richer and more valuable user experiences.

9.2.3 Recommendations and Advertisements

Advertising, when executed effectively, has the potential to significantly enhance the user experience by delivering relevant and desired content. Effective advertising is beneficial because it connects users with products and services they genuinely want or need. Rather than being perceived as a nuisance, relevant advertisements can enrich users' lives by providing information about useful products, new music, upcoming events, or services they might not have discovered otherwise. When advertisements are tailored to individual preferences, they add value to the user experience. This is especially important in a world where there is **infinite content** to consume and our options are nearly limitless.

Spotify's Discover Weekly playlist is a prime example of how personalized recommendations can lead to positive outcomes. Every week, Spotify curates a playlist of songs specifically tailored to each user's music tastes, based on their listening history and preferences. This feature leverages sophisticated algorithms to predict which songs the user will enjoy, resulting in a highly personalized music discovery experience.

For many users, Discover Weekly has become an anticipated event, offering a curated selection of new and lesser-known tracks that align perfectly with their tastes. This not only enhances the user's enjoyment but also supports artists by introducing their music to new audiences. In this case, the recommendation system acts as a form of advertising that users actively seek out and appreciate.

However, current platforms often rely on interpreting implicit signaling of user preferences, which can lead to less-than-ideal recommendations. For example, Spotify's Discover Weekly is based on the user's listening activity over the past week. While this method often provides good recommendations, it does not always capture the user's true preferences.

Imagine a scenario where users could explicitly express their preferences in a universally semantic format that all platforms could ingest. This would eliminate irrelevant ads and recommendations. For instance, users who do not speak Spanish would no longer receive ads in Spanish, and those who prefer House music over Techno would receive recommendations that better match their tastes. By allowing users to explicitly communicate their preferences, platforms would be able to deliver more accurate and satisfying content.

Furthermore, this approach would incentivize users to share their preferences. Users could be rewarded for providing data that helps refine the accuracy of recommendations and advertisements. This creates a mutually beneficial relationship where users receive content that genuinely interests them, and platforms can better serve their audiences.

9.3 AI Implications

Artificial Intelligence (AI) systems are becoming increasingly integral to various sectors, significantly influencing decision-making processes, automating tasks, and driving innovation. However, the efficacy of AI is fundamentally dependent on the quality and integrity of the data it ingests. Inaccurate, unverifiable, or biased data can lead to flawed AI outputs, potentially causing significant negative impacts. Intuition offers a robust framework for ensuring that AI systems have access to high-quality, verifiable, and attributable data, thus enhancing their reliability and effectiveness.

The Intuition protocol incentivizes users to label data in a semantic format, thereby creating a global, permissionless network of actors contributing to a global AI dataset. This decentralized approach aims to serve as the intuition module of the collective consciousness, encouraging individuals to share their information, knowledge, wisdom, and intuition. By signing contributed data with self-sovereign private keys, Intuition ensures that the data is verifiable and attributable, thereby maintaining its integrity.

Verifiable attributes provided by Intuition enable AI systems to also selectively ingest data from trusted sources. Users are motivated to build their reputations to a level where AI companies seek to incorporate their data, potentially rewarding them for their contributions. This system also disincentivizes actions that

Archived copy · cryp2nova.com

could harm reputations, promoting a culture of accuracy and reliability. AI companies may pay for data reads, creating a financial incentive for users to provide high-quality data. The original data creators are thus rewarded, fostering an ecosystem of continuous improvement and trust.

Furthermore, Intuition facilitates the discoverability of private data. AI companies can issue requests to users to run their models over local encrypted datasets, compensating them for selectively disclosing pieces of data or for allowing their models to run using homomorphic encryption/decryption techniques. This approach not only protects user privacy but also expands the dataset available to AI systems, enhancing their learning and predictive capabilities.

10 Conclusion

As we have explored throughout this whitepaper, the evolving landscape of the web is rooted in a fundamental shift from subjective, human-reliant trust mechanisms to more objective, system-driven trust frameworks. This migration is largely being led by decentralized/decentralizing technologies such as those under development in the crypto ecosystem. Despite the remarkable advancements in the development of 'trustless' systems, the broader paradigm of trust remains complex, nuanced, and multifaceted. While trustless systems eliminate certain trust assumptions from the equation of our interactions, even these 'trustless' systems are not fully trustless and are still largely predicated on social consensus and trust in humans. Furthermore, many layers of the decentralized web cannot yet be made 'trustless', and must be made more 'trust**ful**'.

Intuition is envisioned as a solution to help build a more trustful interaction layer of the internet. To accomplish this, Intuition reimagines how data is expressed, structured, refined, and monetized, an innovation only recently made possible through the advancements in the crypto ecosystem. Intuition breaks data down into discrete units called 'Atoms', and encourages the expression of higher-order statements through semantic compositions of these 'Atoms' called Triples. With discrete, referenceable identifiers for all things, value can move through the system programmatically, rewarding users for contributing useful data. Intuition draws inspiration from the game theoretic mechanics that have successfully secured layer 1 blockchains for over a decade, and applies them to the process of achieving consensus around standardized data and identifiers for all things.

The result is an open, permissionless, decentralized social and knowledge graph, built upon the verifiable collective wisdom of the crowds. This can be envisioned as a universal, permissionless, semantic data lake, akin to Tim Berners Lee's original vision of the Semantic Web. The Intuition system serves as a technologically-mediated form of intuition, designed to enhance everyday interactions by providing us all with data we need, when we need it, to better decision-make as we navigate our exponential world.

CRYP2NOVA

Archived copy · cryp2nova.com