Smart Token: The Building Block for the Next-Generation Token-Centric Web

1st October, 2023

Abstract

The evolution of the Web has been marked by significant shifts, from Web 1.0's flat architecture, where the Web was primarily seen as an information repository akin to books, to Web 2.0, where the Web transformed into an application platform. This transformation led to a "reverse pyramid" structure, with contemporary internet behemoths forming the narrow, foundational base. Such centralisation has stifled the Web's innovative potential. As the number of users and websites has surged, the past decade has witnessed a plateau in transformative platforms or groundbreaking innovations, with the digital terrain largely commandeered by a few familiar giants. This paper delves into the root causes of this innovation drought, emphasising the indispensable role of trust anchors in nurturing a vibrant web ecosystem. We introduce the concept of a Token-Centric Web, a vision for the next-generation Internet that decentralizes trust and enables an ecosystem of integrations. In this context, we propose "Smart Tokens," leveraging smart contracts, as an architectural choice to instantiate trust anchors in this Token-Centric Web to amplify user experience, bolster privacy, reduce dependence on monolithic Internet titans, and foster a new wave of web innovation. The paper further probes the potential for transformative shifts across various web dimensions and delineates the technical challenges, potential pitfalls, and adoption hurdles.

Web Foundations: From Information Repositories to Trust Anchors

The Web's Foundational Model

When Tim Berners-Lee and his team developed the foundational concepts of the Web, they selected "sites" as its primary building blocks. This seemingly intuitive approach, however, was not a given, especially when other Internet protocols, like emails and USENET, did not revolve around the concept of sites. Consider USENET: it organises and manages information by topic, making it irrelevant which site or even which planet the information originates from under

that topic.

The Web embraced a site-centric model: a site has a single origin, is inherently competitive, forms an ecosystem through hyperlinks, and evolves as a platform rather than remaining a static product. This model complemented the revolutionary capabilities introduced by HTML, contributing to the Web's rapid adoption and eventual dominance as an Internet application.

Today, with the advent of mobile Internet where sites are often supplanted by apps, the foundational model persists. Although early mobile system designers envisioned apps to be function-centric, akin to desktop word processors and movie players, the reality differed. Instead, users embraced mainstream apps like Google Docs and Netflix. Like a site, a mainstream mobile app possesses a single origin, thrives in competition, links to other apps, and remains open to ongoing development. This evolution is a testament to the enduring influence of the site-based model, even in a landscape that has shifted significantly from Berners-Lee's original vision of the Web.

Berners-Lee and other early web pioneers didn't adopt the "site" concept merely for its potential evolutionary power. Instead, the Web's design was heavily influenced by a prevailing metaphor of that era — the library model, which likened the Internet to a vast library. This metaphor transposed a library's concept—a collection of books—to the digital realm, turning the Internet into a collection of sites. Just as a book references pages, the Web adopted "web pages." This framework led to structuring the Internet around origins (sites) instead of topics (as in USENET) or functionality (as in FTP). Hyperlinks became akin to library indexes, but site owners controlled these links, creating a self-referential mega-book that spanned the entire library.

Structuring the Web around origins rather than topics (like USENET) or functionality (like BitTorrent) had vast implications. It led to websites' single-origin design, reminiscent of how books have specific authors. Today, multi-domain sites are rare. This design choice profoundly shaped our trust paradigm: we often interact with a site based on the trust we place in its origin. A site isn't just an information repository; it represents its origin's credibility.

This decision, to be explored further in subsequent sections, inadvertently paved the way for the Web's centralisation.

The Shift from Information to Applications

Originally influenced by the metaphor of a universal library, the Web was conceived as an information system[1]. Today, such a description feels outdated. A more fitting depiction of the modern Internet is a sprawling network of web applications. Rarely do individuals now describe their online activity as simply "browsing" for information. Instead, they're interacting with dynamic web apps to chat, shop, book hotels, work remotely, network, or even just kill time. Few

[1] Its USENET topic name comp.infosystems.www accurately captured it.

draw parallels between the Internet and a Universal Library these days. The once-prevailing question—how a global computer network might act as a peerless information source, surpassing the constraints of isolated databases or physical libraries—no longer captures the essence of our modern Internet experience.

The transition from a web of information to a web of application marked the significant transformation of Web 2.0. This was achieved by expanding the site model into an application model through web services. Key technologies of Web 2.0 include AJAX, RESTful API, and SaaS. Notably, these are application-oriented technologies built atop the traditional site-based information model. Concurrently, HTML evolved from a document format to an application development User Interface description language. The rise of single-page applications dispelled the notion that the Web is like a book consisting of information pages, suggesting instead a singular page: the application.

This evolution was crucial to understand the trust anchors, which this paper argues played a pivotal role in the centralization of the Internet in the last two decades.

Trust Anchors

Web 2.0 has evolved into a web of applications, each interdependent on a myriad of web services. A mainstream website would typically implement 10-15 mainstream web services such as Google Login and Google Pay.

Unlike traditional application's dependency on system components, these web services transcend their functional roles to become the custodians of trust, safeguarding the secure and reliable operations of web applications. In the discourse of this paper, such pivotal web services are identified as Trust Anchors.

This section will dissect the anatomy of trust anchors, delineate their role in the centralization of the web, and propose a decentralized alternative through the implementation of Smart Tokens. We will start with a definition:

Trust Anchors Trust Anchors are essential web services that web applications depends on, yet can't provide themselves even if they posses the code and computation resources, as it is a point of trust the web applications' business logic depends on. Trust Anchors are culmination of functionality and trust. Trust anchors are web services that offer more than mere functionality; they embody the operational integrity of web applications. Users trust these services having stringent security measures and to remain operational and continue to exist.

The dual-role nature of trust anchor can be explained in a case study

Case Study: Google Login

Two challenges emerge when a user attempts to authenticate with a website. First, the users can't trust that the website can safe-guard their data, such as password. Second, the website can't trust that the user is genuine. This predicament often leads users to prefer logging in with Google, a trusted entity, and websites to favor Google's authentication service. Presently, the reliance on social logins has grown to the extent that some websites have entirely eliminated traditional password databases.

In this context, Google Login serves as a trust anchor, fulfilling a dual role by providing functionality and serving as a bastion of trust. Users trust that Google will adhere to its "promise" of authenticating genuine users without compromising or inadvertently leaking login credentials. A dependency to the centre point is thus created.

While open authentication protocols like OAuth and OpenID allow any website to implement a secure and reliable authentication system similar to Google Login, they typically lack the trust factor necessary to become a trust anchor. A new entity, unlike Google, may not be trusted to maintain consistent behavior, as it could potentially be compromised, deviate from protocol, or cease operations.

Smart Contracts, on the other hand, are bound by predefined behaviors that are not easily altered. Although Smart Contracts can undergo updates, a democratic process such as a Decentralized Autonomous Organization (DAO) can oversee these changes to ensure they do not stray from the original promised behavior, thus maintaining trustworthiness. This paper posits that smart contract-based smart tokens are more aptly suited to fulfill the role of trust anchors, a concept that will be elaborated upon subsequently.

The Limit in the provision of trust Anchor leads to centralisation and innovation barrier

Dr. Gavin Wood has attributed the centralization of the web to a combination of factors. These factors include network effects, economies of scale, big data ownership, and intellectual property laws[2].

This paper posits that the concept of the trust anchor significantly amplifies these factors, coalescing them into a formidable force that cements the centralized stature of today's tech giants like Facebook, Google, and Apple. These providers of trust anchors derive their trustworthiness in reliability and operational integrity largely from their scale and profitability. The rationale is that entities like Google, Amazon, and Facebook have garnered substantial profits by being dependable providers of these trust anchors. Consequently, any deviation from their established behavior for short-term profit is deemed economically irrational.

Such dynamics have exacerbated the centralization within the Web 2.0 ecosystem,

[2]Wood, "The Future of the Decentralized Web."

culminating in an oligopolistic Web 2.0 space.

The trust anchors by the Internet centres, once formed, creates an innovation headwind.

The Trust Anchor Effect: Innovation Stifled by Centralization We define the "Trust Anchor Effect" to the phenomenon where the centralization of trust within a few dominant entities creates a significant barrier to innovation. This effect describes a web ecosystem where new products and services, despite being technically feasible, remain unrealized due to the absence of trust in entities other than the established trust anchors. It encapsulates the dependency on these central points for the provision of trust, without which innovation cannot gain traction or user acceptance.

The trust anchor effect is evident in scenarios where a web service's ability to innovate is contingent upon the trust anchors' willingness or readiness to support new functionalities.

Case Study: Google Pay and Google Wallet

Google Pay, when integrated into web platforms, enables users to complete transactions without directly exposing their credit card details to the merchant's website. Serving as a Trust Anchor, Google Pay extends beyond mere transactional functionality; it is entrusted with ensuring reliability and operational integrity. Even if an open-source developer were to create a feature-wise superior payment system, it lack the level of trust that to function as a Trust Anchor.

With the evolving demands of e-commerce, Google rebranded Google Pay to Google Wallet, expanding its capabilities to store not only credit cards but also items like shopping vouchers and digital car keys. However, these are not made into Trust Anchors.

For example, a website that accepts the shopping vouchers during the checkout process can't use the voucher stored in Google Wallet directly, despite it could with credit cards in Google Wallet. User is required to copy and paste the voucher code, as Google Wallet has yet to develop the voucher as a Trust Anchor service. Similarly, although a user can store a digital car key in Google Wallet, this does not extend to allowing a car cleaning service's website to access the car for service purposes. The user still need to carry a physical car key at the cleaning appointment.

This means any web innovation built on top of the recognition of the shopping voucher and use of digital car key cannot proceed unless Google developed them into Trust Anchor services, creating an innovation dependency.

In essence, the trajectory of Web 2.0 innovation is not solely constrained by the technical ingenuity of developers but is significantly influenced by the strategic priorities of the incumbent Internet powerhouses. The current ecosystem operates under a paradigm where new entrants are beholden to the established trust

anchors, which act as gatekeepers of progress. This dynamic has led to a web landscape that, while ostensibly advancing under the leadership of tech giants, is in fact characterized by a latent inertia. Innovators find themselves in a position analogous to infantry in an army, where their advance is not limited by their own capabilities but by the strategic decisions of the commanding officers. The result is a web environment that is less a meritocracy of ideas and more a hierarchy of trust, with innovation potential tethered to the discretion of a few dominant entities.

The Token-Centric Web: A Paradigm of Decentralized Trust and Integration

The next-generation web, as envisioned in this paper, represents a paradigm shift from the centralized trust anchors of today to a decentralized and integrated ecosystem. This transformation is predicated on the ability to establish trust anchors independently of internet giants, thereby democratizing the web's trust infrastructure. In this chapter, we will explore the implications of this shift, the areas it would revolutionize, and how it culminates in a web defined by limitless integration.

In the current web ecosystem, trust anchors are the domain of a few centralized entities, which has led to a web that is both siloed and constrained by the strategic priorities of these entities. By allowing anyone to develop and maintain trust anchors, the gatekeepers could be removed to enable a web that is more resilient, diverse, and conducive to innovation.

The method of decentralisation of Trust Anchors, Smart Token, will be elaborated shortly, for now let's first look at the implications.

With the removal of centralized control over trust anchors, web services would no longer be limited to integrating a narrow set of core functionalities. Instead, they could leverage a wide array of trust anchors tailored to their specific needs. This would lead to a seamless and cohesive user experience, as services could integrate more deeply with one another.

Missed Opportunities of Decentralised Trust Anchors

Enabling Smaller Trust Anchors

Missed Opportunity: Decentralized trust anchors would allow smaller entities to establish their own credibility mechanisms. This could lead to a proliferation of niche platforms that can cater to specific community needs or specialized markets without the need for endorsement from large internet giants.

Example: In the car insurance industry, small insurers could use decentralized trust anchors to validate car ownership, driver identity, and maintenance records

without relying on cumbersome paper processes. This could streamline operations and allow them to offer competitive rates and services.

Overcoming Barriers to Competition

Missed Opportunity: By removing the monopoly over trust anchors, entities that previously hoarded valuable reputation data would no longer serve as gatekeepers. This would enable a more fluid market where reputational capital can be a portable asset, fostering a more dynamic and competitive landscape.

Example: E-commerce platforms could benefit from a decentralized system where a seller's reputation and customer reviews are not confined to a single platform. This would allow sellers to utilize their established reputation to gain financing or expand their business across various marketplaces.

Facilitating Previously Impossible Innovations

Missed Opportunity: With a decentralized trust anchor system, new services that rely on the integration of multiple trust anchors could emerge. These services would be able to offer highly personalized and flexible experiences that adapt to changing user needs and contexts.

Example: A personalized travel guide service could leverage trust anchors to seamlessly manage and adjust travel plans, including bookings, accommodations, and activities, based on the user's real-time preferences and circumstances. This level of integration and flexibility is unattainable in the current centralized trust anchor environment.

Envisioning the next-generation web

In consideration of the implications previously discussed, this paper proposes a conceptual framework for the next-generation web. This envisioned web is distinguished by the proliferation of ubiquitous trust anchors, which enable limitless and profound integrations across services and platforms. Such a web facilitates a user experience that surpasses the capabilities of the Web 2.0 era and drives innovation forward to enable types of sites and services that couldn't exist prior.

Notably, this vision diverges from the popular concept of Web 3.0, which is characterised as an 'Internet of Value.' Instead, our focus is on the transformative potential of integrations made possible by accessible and universal trust anchors.

Token as the Trust Anchor

The preceding chapter outlined a vision for a web populated by ubiquitous trust anchors. This chapter posits that these trust anchors should assume the form of tokens. We will explore why tokens are suitable as trust anchors, discuss the

technical and layered design implications, and introduce a new design requirement for the type of tokens suitable for trust anchors: smart tokens.

Reflecting on the case of Google Pay/Google Wallet as a trust anchor, one might envision a decentralized trust anchor as a similar entity, such as a hypothetical "DecentWallet." However, this paper argues that the trust anchors should be tokens.

This argument rests on two main premises: one concerning trust, and the other concerning layered design.

Trust Anchors: Tokens, not Platforms

Firstly, regarding trust, we argue that tokens, not software or platforms, are the actual focal points of trust dependency.

Consider previous examples, such as a car key token. If implemented as a trust anchor, it could enable many innovative use-cases. Naturally, questions arise: Should a car wash website accept any car key token authorization and allow the car owner to park the car and walk away? Since many Google APIs are open, one could sign up, create a token called "MyCar," generate a key, and use that on the reservation webpage. The car wash website would accept a non-existent car. Some form of validation must take place.

Two potential solutions arise: the website could maintain a trusted car key token list, or Google could become the gatekeeper, not allowing production car key token releases unless the developer can prove that they are coding the car key token for a genuine car manufacturer. The latter is more practical, so Google becomes not only the car key web service provider but also a curator of valid car key token lists.

However, Google cannot ensure that the car key token functions as the web applications depending on them expect. Each car key token is programmed by their respective car manufacturer, and Google is not in a position to audit their code. Ultimately, the trust lies with the token itself, and Google acts as a transferer of trust rather than the origin of trust. The car wash website essentially trusts that if Google recognizes the car token as being genuinely programmed by a car vendor, such as Tesla, then Tesla would not program their car key token to create invalid authorizations just to spoof the website.

With public key cryptography, it is not a problem to attest that a car key token is programmed by Tesla. Therefore, Google's role is reduced to a curator, and trust remains with the issuer of the car key token, such as Tesla. What makes Google a better curator of valid car keys? They don't produce any cars, nor do they own the knowledge of how each car interacts with their keys.

Recognizing this, a decentralized trust anchor is not the service that makes the token interact with applications - the trust anchor is the token.

Trust Anchors and Layered Design

The second premise concerns the layered design.

The success of the Internet demonstrates the power of a layered approach. The designers of Internet protocol did not concern themselves with what applications and presentations were enabled by the protocol. Instead, they designed it to focus on IP address-based data transfer. This approach allowed for competition among FTP, USENET, and the Web. A layered approach offers an evolutionary advantage. Even if early protocols are not successful, winning protocols like the Web could be designed without reinventing the layers below them.

Continuing with the car token analogy, Google Wallet supports the locking and unlocking of car tokens. If it were willing to enable innovations, it might provide authorization features useful to the car wash company. However, car vendors are the source of innovation in this space. Car vendors could provide functionality to their car keys, such as a car wash mode, or generate geo-fenced keys (car keys that don't allow the car to be driven onto the roads), which the websites could use. But letting Google Wallet decide the features of the tokens would return us to the situation where the whole Web 2.0 market waits for trust anchors to provide certain services in order to innovate.

Therefore, a layered design would be a great evolutionary advantage. Let tokens provide services instead of a platform, and let industrial bodies, DAOs, or applications themselves decide the curated list and standardize the offerings of token functions.

To recap, the two reasons tokens, not platforms, are the trust anchors are because they are the origin of trust, and tokens need to be decoupled from the token-serving platforms such as Google Wallet in order to compete and drive forward innovation.

Given that tokens are the new trust anchors, the effort to decentralize trust anchors should not just decentralize a token-providing platform, but should enrich tokens to carry out the functions of trust anchors. This brings us to the core concept of this paper: smart tokens.

Wood, Gavin. "The Future of the Decentralized Web," 2017.