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 decentralises 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

1

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 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. Even in the mobile Internet era, the foundational model of 'sites' persisted[1].

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[2]. 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 draw parallels between the Internet and a Universal Library these days.

The transition from a web of information to a web of applications marked the significant transformation of Web 2.0. This was achieved by expanding

---

[1]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.

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

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.

As the Web transitioned from an information repository to an application platform, the concept of trust anchors emerged. These trust anchors - essential services the web ecosystem depends on, are usually provided by a few dominant entities and become the focal points of trust for web applications. This dynamic has inadvertently led to the centralisation of the Web, stifling innovation and competition.

Trust Anchors and Web Centralisation: An Unintended Byproduct of Application Shift

The advent of Web 2.0 has given birth to an intricate network of applications, each interconnected and reliant on a multitude of web services. A typical mainstream website might incorporate as many as 10 to 15 mainstream web services, such as Google Login and Google Pay. Unlike traditional applications that depend on system components, these web services have evolved beyond their functional roles, becoming custodians of trust that ensure secure and reliable operation of web applications. In this paper, we refer to these pivotal web services as Trust Anchors.

In this section, we will dissect the concept of trust anchors, explore their role in the centralisation of the Web, and propose a decentralised alternative through the implementation of Smart Tokens.

Trust Anchors: A Definition Trust Anchors are indispensable web services that web applications depend on, even when they possess the capability to provide similar functionalities themselves. This is due to the inherent trust that the business logic of these applications place on these services. Trust Anchors represent more than functionality; they symbolise operational integrity and security, earning the trust of users who rely on them for smooth operations.

Understanding the distinction between a website's functionality and the trust it depends upon is crucial.

Case Study: OpenBanking

To illustrate this point, let's reflect on a case from 2008. One of the authors of this paper, while working with the German Chamber of Commerce in China, conceptualised a website named 'OpenBanking'. OpenBanking aimed to offer superior functionality to existing banking platforms by integrating with the popular Home Banking Computer Interface, providing users with features not available on their banking platforms, such as expenditure pie charts.

Despite its open-source nature and advanced features, users were hesitant to input their credentials into OpenBanking. Interestingly, these same users had no issues using similar functionalities on open-source desktop software. This paradox underscores the importance of trust anchors in user adoption. In this case, the recognised trust anchor was the German bank, and without its explicit endorsement, users were reluctant to trust OpenBanking.

This case study highlights the challenges in establishing new trust anchors and strengthens our argument for the importance of decentralised trust anchors.

Case Study: Google Login

When a user attempts to authenticate with a website, two challenges arise. Firstly, users often doubt the website's ability to safeguard their data. Secondly, the website may struggle to verify the authenticity of the user. This predicament often compels users to prefer logging in with Google, a trusted entity, and websites to adopt Google's authentication service. Currently, the reliance on social logins has grown to such an extent that some websites have entirely eliminated traditional password databases.

In this scenario, Google Login serves as a trust anchor, providing functionality and acting as a beacon of trust. Users place their faith in Google to authenticate genuine users without compromising or inadvertently leaking login credentials. This creates a dependency on a central point.

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 behaviour, as it could potentially be compromised, deviate from protocol, or cease operations.

The case studies above help us to better understand the characteristics of Trust Anchors.

Characteristics of Trust Anchors

1. A trust anchor is an essential dependency, not just a popular service. For example, Google Analytics is not a trust anchor, as a website can carry out its own analysis. Its popularity is based on traditional factors of centralisation like big data, network effect, and IP laws, not on its role as a trust anchor.
2. A trust anchor is trusted to follow a protocol and is expected to not betray the trust.
3. A trust anchor elevate user trust to meet the demand of the application. For instance, users willingly provide their credit card details to Google Pay for transactions on merchant websites. However, not all service providers act as trust anchors. For example, Amadeus, which provides flight data

and reservation services for airlines, operates in the airline website's back office without needing to elevate user trust.

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

Dr. Gavin Wood has attributed the Web's centralisation to a combination of factors. These factors include network effects, economies of scale, big data ownership, and intellectual property laws[3].

This paper posits that the concept of the trust anchor significantly amplifies these factors, coalescing them into a formidable force that cements the centralised 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 behaviour for short-term profit is deemed economically irrational.

Such dynamics have exacerbated the centralisation within the Web 2.0 ecosystem, 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 Centralisation We define the "Trust Anchor Effect" as the phenomenon where the centralisation 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 unrealised 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.

---

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

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 characterised 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.

Reimagining Web 3.0: Beyond the Internet of Value

The prevailing vision for Web 3.0 is characterised as an 'Internet of Value.' This perspective sees the next-generation Web as a platform where value, in its various forms, is distributed more equitably among users and creators, breaking away from the monopolistic tendencies of the Web 2.0 era. The centralisation of value, in this view, is seen as the root cause of many of the issues plaguing the current web ecosystem, from stifled innovation to privacy concerns.

However, this paper proposes a different interpretation of the evolution from Web 2.0 to the next generation web after it. Rather than viewing the centralisation of value as the *cause* of the Web's current challenges, we argue that it is, in fact, a *consequence* of the Web's evolution. The transition from Web 1.0 to Web 2.0 was not primarily driven by a pursuit of centralised value, but by the desire for more dynamic, application-oriented experiences. Therefore, it is not logical to assume that the transition to Web 3.0 should be defined by a reversal of this trend.

Moreover, the idea of Web 3.0 as an 'Internet of Value' may reflect more of a wishful thinking than the actual evolutionary process of the Web. Not everyone who moved to Web 2.0 was pursuing value, and not everyone who moves from Web 2.0 to Web 3.0 will be pursuing value either. The value investing community, while growing, still represents a small section of web users, and it is likely to remain so in the future.

Instead of defining Web 3.0 as an 'Internet of Value,' this paper proposes an alternative vision: the 'Next-Generation Web.' This Next-Generation Web shifts focus from the distribution of value to the decentralisation of Trust Anchors, attacking the root cause of centralisation while continuing to progress in the demand-driven direction that has been driving the Web 1.0 to 2.0 upgrade. This perspective views the Next-Generation Web as a platform that fosters widespread innovation and enables more profound integrations by allowing anyone to develop and maintain Trust Anchors.

The Trust Anchors of the future Web will not be platforms or services, but tokens - specifically, Smart Tokens. The ensuing sections will delve into this concept in more detail.

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

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

In the current web ecosystem, trust anchors are the domain of a few centralised 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.

With the removal of centralised 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

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 decentralised system where a seller's reputation and customer reviews are not confined to a single platform. This would allow sellers to utilise their established reputation to gain financing or expand their business across various marketplaces.

Facilitating Previously Impossible Innovations

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

Example: A personalised 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 centralised trust anchor environment.

Enabling Long-tail Trust Anchors

Missed Opportunity: Decentralised 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 specialised markets without the need for endorsement from large internet giants.

Example: In the car insurance industry, small insurers could use decentralised 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.

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 decentralised 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 authorisation 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 recognises 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 authorisations 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.

Recognising this, a decentralised 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 for tokens being trust anchors concerns the layered design of the Internet. The success of the Internet demonstrates the power of a layered approach. Instead of designing protocols around specific applications, Internet Protocol designers focused on enabling IP address-based data transfer. This approach allowed for competition among various Internet applications, such as FTP, USENET, and the Web, and provided an evolutionary advantage. Even if early protocols failed, more successful ones like the Web could be designed without reinventing the lower layers.

This layered design approach can be applied to our car-key token analogy. Google Wallet, for example, supports the locking and unlocking of cars using car-key tokens. To enable innovations, Google Wallet could potentially provide authorization features useful to a car wash company. However, the real source of innovation in this space is the car vendors. They could add functionalities to their car-keys, such as a car wash mode or geo-fenced keys that restrict the car from being driven onto roads.

If Google Wallet were to dictate the features of the tokens, we would revert to a scenario where the entire Web 2.0 market waits for trust anchors to provide specific services before they can innovate. A layered design, where tokens provide services independently of platforms like Google Wallet, would offer a significant evolutionary advantage. This approach would allow industrial bodies, DAOs, or applications themselves to decide on the curated list and standardize the offerings of token functions.

In conclusion, tokens, not platforms, should serve as trust anchors for two reasons. First, they are the origin of trust. Second, tokens need to be decoupled from token-serving platforms to foster competition and drive innovation. Therefore, efforts to decentralize trust anchors should not just focus on decentralizing token-providing platforms, but also on enriching 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.

10