YINC: An escrowed platform for service providers and consumers, with tamper proof reviews.

Jaime Bemaras, MSEE

Abstract

A platform for facilitating contracting and payments between service providers and consumers is described. The platform is configured to elicit multiple competitive quotes from service providers for a given work assignment. Flexible payment schedules for a given work assignment are supported, via an intrinsic escrow system based on a cryptocurrency token. A cryptographically attested system for public, tamper proof reviews of completed work assignments based on smart contracts is also provided by the platform.

Table of Contents

1 Service Provisioning

1.1 Electronic Wallet Registration

Both service providers and consumers require registration in the YINC platform. When a user (regardless of kind) registers, part of the process may involve the creation of an electronic wallet to hold the user's YINC tokens if the user does not yet have one.

A necessary step in the registration is to provide YINC with the wallet's public key. A public key to a user's electronic wallet is indispensable for processing payments and refunds via the YINC platform.

1.2 Submission of a Work Assignment

Once registered, a service consumer can submit work assignments through the platform and open them for quoting by service providers.

1.3 Provider Selection via Competitive Bidding

Upon submission of a work assignment, the platform automatically invites service providers to bid for the assignment. This is an excellent source of immediate, legitimate and continuous leads for local service providers.

Bids are viewable by both the consumer and interested providers, with one important difference: service providers can only see which other providers have bid on an assignment; not the amount quoted to the consumer. This allows the consumer to compare provider's quotes, and offers providers an opportunity to revise their quotes if they so choose. It also creates a sense of urgency among the bidding service providers, who want to win the consumer's business before more providers submit their quotes.

The platform provides ways to communicate directly between the consumers and providers, allowing the consumer to make a more informed choice of providers, beyond a mere quote comparison.

The consumer is empowered to examine provider's past reviews of work assignments, to help them gauge the responsiveness, professionalism and workmanship of potential providers. Armed with information, the consumer can now make an informed selection, negotiate the terms, and grant the work assignment to their provider of choice.

Service providers are also empowered to examine the consumer's past reviews of work assignments completed for them, for example to gauge if they are objective in their reviews and subsequent comments. Service providers interested in a particular work assignment are predicted to be more proactive in their communications with potential and fair clients because of the competitiveness of the bidding process.

1.4 Escrowing

Payment terms are dictated and agreed upon by both parties for each work assignment. The platform supports payment for retainers and milestones in any combination, thus providing an extremely flexible and individualized payment schedule for any kind of assignment.

YINC tokens are used as the exclusive peer-to-peer payment vehicle throughout the platform. All payments and refunds to users are paid using YINC tokens.

The platform also supports unbiased mechanisms for disputes and arbitration, in case a work assignment is left incomplete, or the parties disagree on the outcome of the work performed.

2 Blockchain Attested Reviews

Upon conclusion of a work assignment via the platform, both the provider and the consumer are given the opportunity to write and publish a review of the assignment. Reviews are allowed on concluded assignments only, and only by the users directly involved with the assignment.

YINC leverages the distributed and immutable nature of a public blockchain to guarantee the authenticity of its user's reviews, using a patent-pending approach. All reviews are permanently available to the public, and it is easy to verify whether a review has been tampered with since its publication.

2.1 Structure of a Review

Reviews use a light markup language (e.g., YAML) to structure and store their contents in a journaled document.

Each review begins with a header entry that includes:

- an entry separator
- the review's structure format version (all subsequent entries must adhere to the same version of the review's structure)
- a unique identifier for the work assignment

- its contractual start date

The reviewer's initial entry and any subsequent comments follow, using an extensible and versioned structure. Each entry's structure includes:

- an entry separator
- the work assignment's unique identifier
- a sequence identifier for the entry
- a timestamp for the entry
- a previous entry referencing identifier, for threaded responses
- a content advisory field, to flag entries complying or not with a particular edition of YINC's review guidelines
- the entry's text

The reviewer is also able to insert into their entry one or more links to URIs with supporting content (e.g., audio, photos, videos) hosted elsewhere. The entry itself only stores the links to the supporting contents, and they are neither verified, downloaded or incorporated into the review by YINC. YINC thus segreagates itself from content ownership claims. See also 2.4 Content Ownership and Identifiability for additional information.

2.2 Public Availability

Reviews and their subsequent comments are stored as individual documents using Distributed Version Control System (DVCS) repositories. YINC makes these DVCS repositories available to the public at large, in Read-Only mode.

Each reviewer's entries are appended to its corresponding review, and committed to exactly one of YINC's public DVCS repositories. Each document in a repository contains all the entries of a single review.

Anyone is welcome to duplicate the repositories in whole or in part at any time, and to also make them available as safety copies to others. However, the only authoritative reviews are those made available to the public in YINC's DVCS repositories.

YINC initially uses a separate repository per year. Depending on the volume of reviews, YINC may choose to use instead individual repositories for each year's sub-period (i.e., quarter, trimester, month or week,) to maintain data sizes manageable. Separate repositories per year or

year's sub-period naturally provide a more manageable data warehousing strategy. However, since anyone can duplicate any repository at any time, data is expected to outlive any such strategy outside of YINC's public repositories.

2.3 Tamper Proofing

A requirement for the DVCS in use by YINC is its widespread availability to the public. Anyone should be readily able to duplicate any of YINC's public repositories, and gain immediate and unfettered access to all its reviews, independent of the user interfaces that YINC makes available to the public at large. This unfettered access is crucial to empowering anyone to corroborate that all reviews are both authentic and unmodified.

Another requirement for the DVCS is that it produces a unique enough hash for each commit. The leniency on hashes not being strictly unique is inherited from widely used and publicly available DVCS systems, like Mercurial and Git. A discussion on the choice of a particular hash and its expected uniqueness is both out of scope for this document and well covered by the tools themselves. For YINC's purposes, they are deemed distinctive enough to be used as unique identifiers for the journaled contents of each review.

However, the DVCS-generated hashes are not enough to fully guarantee untampered reviews. There is no way to reliably ensure that a particular repositoty's history has not been branched and merged, amended, re-written or otherwise altered solely from its hashes. A reliable and unalterable mechanism, separate from the DVCS repositories is thus required.

YINC uses smart contracts in a publicly available blockchain for such a mechanism. YINC relies on the widespread availability, distributed nature and inability to modify a smart contract's transactions running on a public blockchain to attest that every entry in a review is unaltered since publication.

Once the reviewer submits their entry for publication, the smart contract permanently records essential information on the blockchain, including:

a) the repository's name

b) the commmit's hash.

c) a digital signature of all the contents of the review up to that point, including the reviewer's latest entry, generated by the reviewer's private key.

d) a digital signature of all the contents of the review up to that point, including the reviewer's latest entry, generated using one of YINC's private keys.

Once the smart contract is fully executed and recorded in the blockchain, its data can be easily retrieved. The commit's hash from the retrieved data uniquely identifies a particular commit in a published repository, and both signatures from the retrieved data can be easily verified using the contents of the commit and the public keys of both YINC and the reviewer.

This simple validation of the signatures thus ensures that both, the contents of the review have remained intact, and that no one can ever modify a copy of a repository without rendering that review invalid in that copy.

It is important to emphasize that to enforce immutability, each entry in a review and its signatures reside in completely separate and independent data stores. Therefore, as separate data, each can be designated as:

D_{RE} – Review Entry Datum

D_{ESR} – Reviewer's Entry Signature Datum

D_{ESY} – YINC's Entry Signature Datum

However, since the review's entry is related to both mutually independently signatures, it is convenient to think of the entry's data as a single, logical set of information; a single entity, regardless of how many copies of the same information exist[1].

Thus, an entry (and each of its identical copies) can be designated as the set:

$$E = \{D_{RE}, D_{ESR}, D_{ESY}\}$$

The fact that each digital signature covers not only the latest, but also every prior entry in the review up to that point, intrinsically creates a traceable signature history of every entry in a review. Conceptually, the latest entry is composed of its own contents as well as of all entries that came before it:

$$E_n = \{E, E_{n-1}, E_{n-2}, \ldots E_{n-m}, \ldots E_0\}$$

And the set of all existing and related entries represents the latest state of a review:

$$R = \{E_n, E_{n-1}, E_{n-2}, \ldots E_{n-m}, \ldots E_0\}$$

It is not mandatory, however, to evaluate every digital signature associated with the review's history to determine if a review has been altered in any way. Because it can be recursively

1 Recall that multiple copies of each entry in each review in the authoritative YINC DVCS repositories are expected to exist beyond YINC, and that every copy of the public blockchain will carry within it the entries' signatures.

proven that every prior entry in a review has remained unaltered via its digital signatures, and the latest digital signatures cover the latest as well as all previous entires, it should therefore be enough to verify only the latest signatures to establish that the entire review has remained unaltered. Hence:

E_n is valid **iff**[2] D_{ESR} corresponds to D_{RE} and D_{ESY} corresponds to D_{RE}

but

E_{n-1} is valid **iff** $(D_{ESR})_{n-1}$ corresponds to $(D_{RE})_{n-1}$ and $(D_{ESY})_{n-1}$ corresponds to $(D_{RE})_{n-1}$

therefore

R_n is valid because $\{E_n, E_{n-1}, E_{n-2}, \ldots E_{n-m}, \ldots E_0\}$ are all valid

2.4 Content Ownership and Identifiability

Each reviewer is responsible for their reviews and subsequent comments, and owns all rights to them. YINC does not claim ownership of, or responsibility for its contents.

Reviews are never anonymous – they are intrinsically and permanently associated to the keys of a user's wallet, as discussed in 2.3 Tamper Proofing.

2.5 Compliance with the Code of Conduct

Reviewers are expected to strictly adhere to YINC's latest published Code of Conduct at all times when writing their entries. Once a reviewer submits an entry, YINC may choose to inspect the entry for compliance. If the entry does not comply with the current Code of Conduct, YINC may alert the reviewer and give them the opportunity to edit their entry, or to confirm that they want to submit it as is. If the submitted entry is not compliant – in YINC's sole criteria, YINC may flag that entry as such. Refer to the entry's structure in 2.1 Structure of a Review.

YINC cannot modify what a reviewer submits as the contents for an entry without invalidating the user's digital signature for the entry. However, YINC does reserve the right to note an entry as non-compliant, and to redact or entirely omit non-compliant reviews from its user interfaces. The partial or full exclusion of a review from YINC's user interfaces does not alter the contents of the publicly available reviews. And any exclusion or redaction is clearly marked as such in YINC's user interfaces.

2 See http://mathworld.wolfram.com/Iff.html

2.6 Caching and Searching

In order to provide the fastest and most convenient access to reviews, YINC also commits every review to databases exclusively controlled by YINC, and only available to the public via YINC's public interfaces.

Once a reviewer's entry is submitted for publication, the exact same contents are simultaneously recorded in a publicly accessible repository (as discussed in 2.2 Public Availability) as well as to YINC's internal databases. The same signatures computed for inclusion in the entry's smart contract are stored along with the journaled entries in YINC's internal databases, and can be used to cross-verify the review's integrity in the exact same way (see 2.3 Tamper Proofing).

In addition, YINC maintains several indexes to make it easier and faster for its users to find related reviews. For example, it ought to be possible to find all the reviews from a particular user, or all the reviews for a particular service provider, or all the work assignments linked to a particular address.

It is this last feature that intrinsically provides a searchable and immutable account, for example of work actually completed by a particular service provider and at a particular address, which could be used as an public electronic record potentially spanning decades.

3 Platform Specializations

3.1 Referencers

Once a consumer writes a review for a concluded work assignment, YINC may provide the opportunity for the reviewer to also become a referencer in the platform. The platform may incentivize the reviewer with additional tokens for every instance where the reviewer agrees to be a live source of information to other potential clients regarding the provider they reviewed, regardless of whether their experience with that provider was favorable or not.

3.2 Commercial Real Estate

YINC may provide a customized platform, specifically for the needs of commercial real estate. A service management tool would allow tenants to make requests directly to their management team for repairs or services. Property owners and managers would then have the ability to use the YINC platform for jobs they want to offer to YINC vendors, as well as jobs that their own in-house or preferred vendors can handle, including small tasks their building manager or super can complete without the need for an external service provider. Reviews of these work assignments may not be available beyond the tenants, property owners and managers.