YOOPING

Evolving communications with blockchain & smart contracts

Draft White Paper

Version 1.1 - 13th February 2018

Important Disclaimer

This document is a draft and is provided for information only. The information contained herein is subject to change and does not commit YOOPING, it's owners, intellectual property holders, executives or related parties in any way. The final version of the proposal will be published as soon as adopted.

Aim

To introduce a platform that allows everyone to maintain their own communication preferences and allows services to interoperate with them, based on a few simple terms:

i) “Accept” - The user will accept communication from the sender.
ii) “Reject” - The user does not accept communication from the sender.
iii) “Fee” - The user accepts communication for a user defined fee, allowing the sender to decide.

Table of Contents

Business Case

We aim to give every entity (person, business, bot etc) the ability to control who can communicate with them and on what terms. Using blockchain technology and smart contracts we give the existing communication industry (our partners) “trust” outside of their own networks.

Using a secure, lightweight protocol we aim to let everyone control or prevent unsolicited telephone calls, emails and other digital communication (including social media, instant messaging and gaming). Entities may also control who can consume their content and on what terms.

This is achieved by four core components:

1) A decentralised, encrypted user preference registry
2) An escrow service based on smart contracts
3) The sender APIs (Application Programming Interface) and protocol
4) The receiver APIs (Application Programming Interface) and protocol

Collectively, this is known as the YOOPING platform. Ultimately, YOOPING’s design and future development will be shaped by a consortium of Communication Providers, run to benefit all the participants in the industry.

We need this because, although communications have improved massively, aiding our social, educational and economic requirements, the industry is still flawed. For example, it is estimated that email spam costs the global economy $50bln annually. Phishing is another way criminals try to gain access to knowledge or value, this time using telephony.

It would be easy for individual providers to build a trust system within their own networks, but it doesn’t work when communications are between entities using different providers.

Even on a single provider’s service where trust could be established, the recipient is rarely in control. Instead, the recipient is subjected to advertising as a way for the service to be monetised. Content creators cannot control the value they put on their own time, instead having to adhere to advertiser friendly algorithms and the impact of occasional “admegeddons” (where the algorithm changes and affects their income).

We propose to put the recipient in control. To let them decide how they participate in any bi-directional digital communications and on what terms. Let people value their own time. Through a decentralised user registry, lightweight API & protocol and blockchain technology utilising smart contracts, we believe we can innovate the communication industry, to the benefit of users and providers, spurring the development of the next generation of communications and interoperability. We can help prevent fraud and crime and help protect society by eradicating digital spam and phishing. We can reduce cold calling and marketing calls or allow people to choose to be paid to receive them. We can stimulate new income for digital content producers

and anyone who feels people will pay to contact them (businesses, advisors, celebrities) controlled by the user setting their own fee, not having one imposed upon them.

How it Works

Any communication sent to a compliant application (or device) uses our decentralised registry to determine the user's preference. In order to send an initial (or unsolicited communication), the sender risks paying a fee (via a smart contract) which may result in a loss or a refund. The addition of an upfront fee immediately makes spam uneconomical and helps eradicates it. In order to check a recipient's preferences, the sender must be known (and can be identified by the recipient). This renders phishing less of a risk. Once a user is in control of their communication preferences, a whole new economy is created as we are, in effect, letting users define their own digital stamps or telephone exchange fees. Marketing becomes more accurate as people can set a price for which they will tolerate it and therefore valuable, targeting willing or paid participants, rather than the shotgun approach of today.

Why a problem exists

Communication has evolved rapidly through technology. We now have so many ways we can receive information, whether or not it is requested. However, with unsolicited information comes the risk of fraud, spam, phishing, crime and the cost of these is estimated to exceed $20bln annually ([1]) in the US alone and $50bln globally. The three main reasons why nothing has been done are:

1) Security - early communication, such as telephone or email did not guarantee the sender's identity. The consumer had to receive the communication and trust the identity. This led to widespread spam, phishing and fraud. It is estimated that over 58% of email is spam ([2]) and in an Ofcom study, 83% of participants reported a nuisance call at least once in a 4 week period [3]
2) Financial - levying fees, especially micro-payments are uneconomical given the current payment providers who normally have some minimum transaction cost (20c) and a percentage. This makes message sending cumbersome to bill in bulk or too expensive to send individually. Refunds and queries are too time consuming to maintain.
3) Commercial - providers of communication services make money from each communication event, or advertising or data mining of information for providing the service. It is not in their interests to discourage users from using their products or limiting the messages they send.

[1] CMSWire - https://goo.gl/zbJ832
[2] Statista - https://goo.gl/mEBjk7
[3] Ofcom - https://goo.gl/a1Sb6W

So, how can we change anything when security, financial and commercial reasons prevent us from doing so? The answer lies in the innovation of blockchains, de-centralised services and cryptocurrency. These technologies have incredible power to resolve problems and they provide ideal filips for the problems associated with digital communications:

1) Security - blockchain works by decentralised trust. Encrypted account data (never exposed publicly) can be mapped to public addresses to assure identity, ensuring the sender and recipient are internally known. Using signed tokens, read by the recipient, security and non-repudiation concerns are addressed.
2) Financial - Smart contracts and cryptocurrencies can perform micropayments based on conditional logic. Valid communication can be sent for free, whilst unsolicited communication can have a conditional fee levied. If the communication turns out to be acceptable, the fee can be refunded for a fraction of the cost of traditional payment processors. Imagine, if every spammer had to pay 25 cents to send a spam email? It would be uneconomical and the problem is solved.
3) Commercial - Users want better products and will use the applications that give them control with revenue generated by communication, not just advertising. We are not advocating removing advertising, but we introduce a new payment source, which the communication partners can share by integrating the platform.

The Solution

Innovation has driven change

Blockchain technology and smart contracts have created a platform which decentralises, adds trust and consensus and allows value movement (payment or refunds) based on rules. We can now overcome the three reasons why users can't control their own communication preferences.

High Level Overview

For the purpose of the overview, YOOPING comprises 4 main topics:

1) The User Registry Service - a secure, encrypted registry with public APIs
2) The Escrow Service - a Smart Contract service
3) The Sender - a protocol any "sending" application or device must adhere to
4) The Receiver - a protocol any "receiving" application or device must adhere to

Interaction occurs between:

1) The Sender and the Registry
   Communication is performed using an HTTP Restful Interface

2) The Registry and the Escrow Service
   Communication is performed using an HTTP Restful Interface

3) The Sender and the Receiver
   Communication depends on the connecting application or devices. It can be a web protocol (for example a social media application delivering an event), telephony based (for a phone call) or near field(in the case of a beacon and phone). The recipient does not need to contact the registry again as a signed token will allow it to trust (or reject) the sender's communication.

4) The Receiver and the Fee Engine
   Communication is performed using an HTTP Restful Interface

Roles

User - an entity who defines a communication preference
Partner - a commercial entity implementing the protocol

The User Registry Service

We introduce a global user preference registry, in which users can define their communication preferences in a tree structure either globally, per communication type or per sender. For example, I could decide my default preference is to reject all communication, except phone calls, from my family (a collection of 5 telephone numbers). The registry entries are encrypted using my key, so data is not publicly visible.

The registry exposes some Restful APIs which allow Senders and Recipients to interoperate.

The Escrow Service

A service that manages the creation and lifecycle of smart contracts. The Escrow Service generates an identifiable token which the receiver will check before accepting a communication. If the communication is subsequently delivered, the recipient can determine whether or not to enforce the fee (the important point is the fee is held in escrow in advance). The fee used by the escrow service is the YPNG coin (or a token derived from it should the ETHEREUM network not be performant enough), which all senders need to purchase, in order to send messages to recipients whose preferences require a fee to be sent. Therefore, the YPNG utility token, offered in the Token Sale, will be the only way senders can arrange for messages to be sent.

The Sender

The Sender can be an Email client, a Messaging service, an HTTP service (such as a banner ad provider), a Telephone (or mobile handset) etc. The sender protocol is implemented by our partners within their applications or devices (we shall see why later). We will also create our own commercial implementations, the easy of which being an Email alternative.

The sender application calls the Registry using an API, supplying the recipient's public address (an email, a phone number etc) and their own credentials, to checks the recipient's preference. The response to the call determines what it does next.

- Proceed with the communication
- Cancel the communication
- Enquires with the user if they would like to continue (as a fee may be required)

The Receiver

The Receiver is the same type of application or device as the Sender (an Email client, a Messaging service etc). Once again, the protocol is implemented by our partners (except for our own commercial offerings).

The receiver checks a JWT (JSON Web Token) sent with the communication to see if it is:

- Trusted
- Un-tampered
- Fresh

The communication is received and, if the user's preference meant a fee was levied for delivering the communication, the receiver can now enquire how the user wishes to proceed.

The decision to refund or collect the fee is sent to the Escrow Service and the smart contract is processed accordingly, either returning the fee to the senders wallet, or distributing it between the recipient and the partner.

Important Note**!** - both the "User" and "Partner" generate revenue from the YOOPING service incentivising adoption and innovation.

Legacy Connectivity

Sender Application	Receiver Application	Receivers behaviour
YOOPING Compliant	YOOPING Compliant	User Preferences
Legacy Device	YOOPING Compliant	User Preference defaults
YOOPING Compliant	Legacy	Always receives

Analogy

Letting users control their own preferences and setting the value of contacting them is like letting them print their own stamps, or set their own phone tariff. It not only deters unsolicited communication, but could drive significant innovation in the communications industry, spawning economic benefits to a wider audience.

Standard User -

Charge 50p for all communication
Except the following email addresses (no extra fee)
Except the following telephone numbers (no extra fee)

Business User -

Charge £10 for my clients to call me
Charge £20 for unsolicited calls
There's no charge for my friends
Charge £1 to email me

Vlogger - “Let me know what great product you want me to consider reviewing next”
Charge £0.25 per subscriber’s instant message

Scope - the digital communication ecosystem

Anything that we can receive through a digital medium can be thought to be part of the digital communication ecosystem:

- Email
- Fixed line telephony
- Mobile telephony
- App Notifications
- Voip / Sip
- SMS / Text
- Social Media
- Messaging Services
- IPTV
- Online content producers
- Online Media companies
- Near field
- GPS & Digital Audio
- Banner Advertising

Some of these services can be addressed quickly. For example email is a quick win. Nuisance calling and telephony can be changed fast, as their is commercial advantage for handset manufacturers to share revenue from a user defined tariff. Messaging and some social media can be fast adopters, as a meaningful revenue stream is unlocked by micropayments and cryptocurrencies.

Others, who are based on legacy advertising revenue for their large incomes and expenditures may take longer. However, the benefit to marketing companies knowing the real “eyes” on advertising (as they are incentivised to watch it) versus the current un-targeted approach may force adoption from the vendor rather than the consumer perspective.

Benefits of the YOOPING Platform

User Benefits

Most people receive unsolicited communications they would prefer not to. Having an easy, default way to reduce this is a good start. However, without always knowing the source, we may not want to reject everyone. Therefore, having an easy way to control future communication by

sender (either by specific type or all types) empowers people. That's why YOOPING provides such a simple, fast, protocol.

Social Benefits

People, especially vulnerable or non technically aware are especially susceptible to spam and fraud. Through sensible defaults, these people are protected by an initial communication fee which deters spam and even marketing companies from contacting them.

Economic Benefits

The reduction of spam and phishing will save the global economy up to $50bln annually. The communication between businesses and consumers will be more trusted, leading to better sales and less fraudulent transactions.

Commercial Benefits

Competitive advantage is key to most businesses and disadvantage actively reduces product effectiveness. Therefore, as users want more control, they will migrate to products that give them the benefits, creating churn in services which don't. We believe our industry bodies, which will derive the protocols per communication type, will be popular with all of the largest commercial product producers, as they will have a vested interest to implement their users requirements as seamlessly as possible.

The other benefit partners will revenue opportunities. Although some may currently make money supporting unsolicited communication events, we believe giving the users the ability to control their own contact fees will, ultimately profitable revenue streams for all of our partners and stimulate further innovation in the communications industry.

Governmental Benefits

Governments save tremendous amounts of money which had been spent on complaint handling and criminal investigations, trying to identify and prosecute the beneficiaries of spam, phishing and fraud.

Innovation Benefits

Imagine a world where you can charge an individual or group, any fee for communicating with you, if they are willing to pay it. Already applicable to businesses, knowledge workers, celebrities and digital content producers (such as blogger and gamers) who can immediately unlock a source of revenue and monetise their work. Now think of the potential for other people to kickstart a career or business by offering paid advice or help. These new innovators stimulate the economy and advance innovation in communication further. Tax on each transaction is sourced automatically, helping the social bill. The future is exciting when you think about it. By decentralising user preference and decentralising monetisation, justifying the importance of cryptocurrencies, communications could be the catalyst for innovating business of the future.

Security / Protection from abuse

Security is paramount for both senders and receivers. Digital Signatures linked with cryptocurrency accounts give us a high level of protecting our users' details. The sender needs to know the public address of the recipient but in return exposes their own public address. We also track their account which we, by default, operate under a fair use policy. We handle abuse in 2 ways:

i) If usage looking up a recipients exceeds a predefined limit, their responsiveness deteriorates and can time out. If this is associated with a commercial product, the partner should contact us to negotiate a new policy, based on users (which in turn will feed back into their industry membership fee).
ii) When the API is called, we generate a transaction id which has a time to live (reflecting users change their preferences). So even if the details of a user were mined for a marketing database, anyone trying to initiate communication with an expired transactionId would be rejected at source and lose their fee.

Reference Implementations

In order to kickstart commercial partnerships, we aim to create commercial implementations supporting the YOOPING Platform as follows:

- YOOPMail - Email hosting using YOOPING platform
- YOOPSnoop - Streaming service for content creators
- YOOPChat - Instant Messaging
- YOOPCall - Telephony
- YOOPSocial - Social Media

Value Proposition

Senders

At the heart of the system is the commitment to risk a small fee to deliver communication, which discourages unsolicited communication. Subsequent communication may be free (if the recipient accepts) but there is also the potential a rejection or fee is established. In all cases except an established “accepted” preference,

The default email fee will be set to the equivalent PING$ of $0.5, £0.5, €0.5. However, the user can change or remove this.

Initial Revenue Matrix (under advisor review)

Application	INITIAL ACCEPT[4]			REJECT			FEE		
	U	P	Y	U	P	Y	U	P	Y
Email	-	10%	5%	70%	25%	5%	75%	20%	5%
Fixed Line	-	0%	5%	70%	25%	5%	75%	20%[5]	5%
Mobile	-	0%	5%	70%	25%	5%	75%	20%[6]	5%
Social Media	-	10%	5%	70%	25%	5%	70%	25%	5%
Messaging	-	10%	5%	70%	25%	5%	70%	25%	5%

U - User, P - Partner, Y - YOOPING

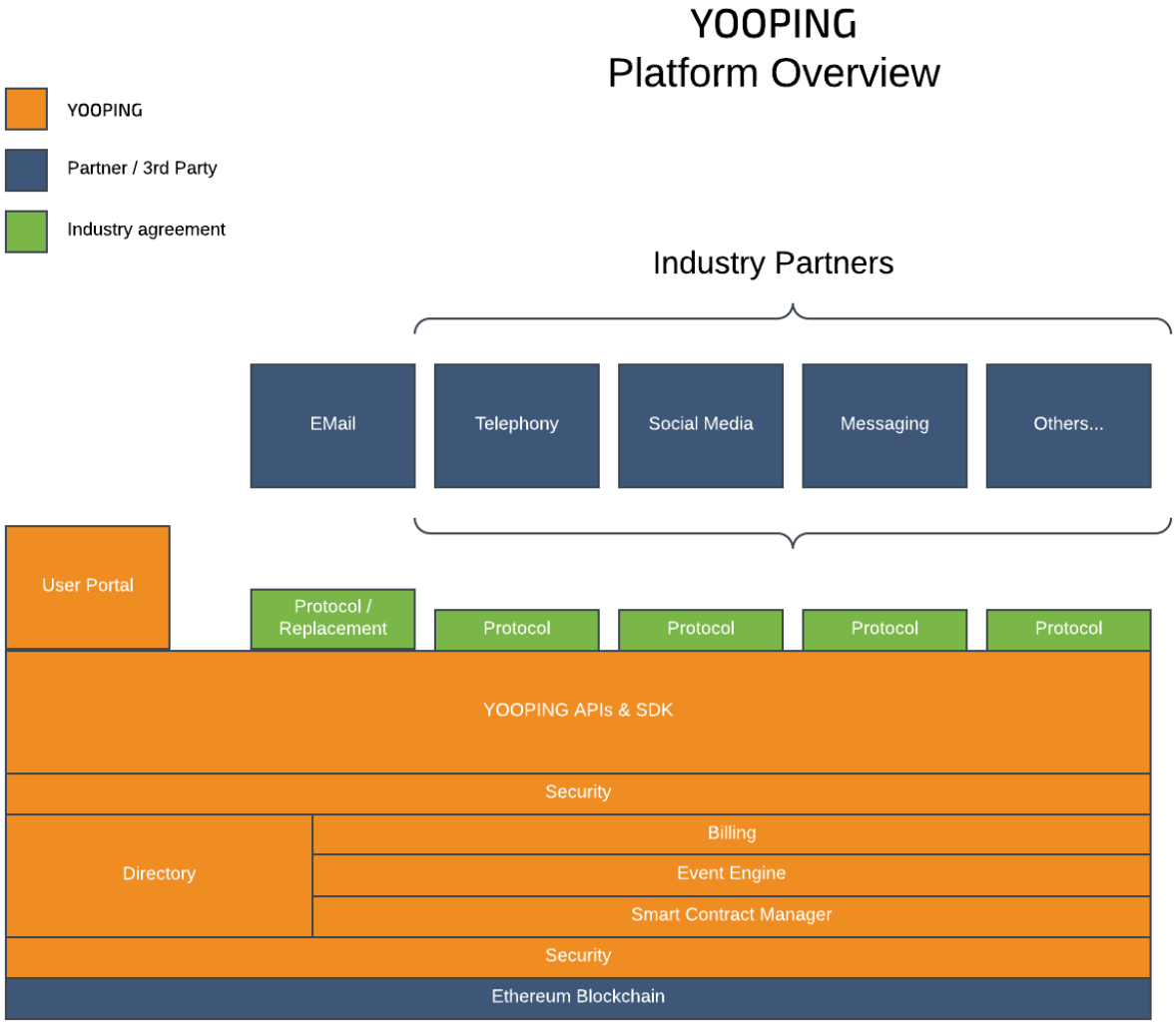
[4] Where user decides to whitelist sender
[5] Telephony partners are also generating revenue from the call.
[6] Telephony partners are also generating revenue from the call.

Token Offer

Should you be interested, please see our website for more details: https://www.yooping.com

Technical Overview

The Platform



The platform is designed to give users a simple environment for managing their communication preferences. It also is backed by a technology stack that emphasises security, ensuring senders and receivers have an identity (although only the public version is exposed) allowing preferences to shared. The platform has default fees which discourage unsolicited communications, but allow the users to change these for any communication type or even individual sender. Unsolicited communications that are received can be rejected and the fee kept, or they can be accepted at which point the fee is refunded. All of these billing operations

happen in the background, automatically, letting users enjoy communications without large administration overheads.

Simple, Lightweight, Extensible Protocol

For efficiency, the YOOPING platform has been designed to be fast and lightweight. It relies upon an API challenge which returns a JWT (that is signed). This means, one API call is initiated at the sender, but the recipient can make a decision without a network call.

Users have a simple portal where communication preferences can be set using standard browser technology. Sensible defaults are applied for all communications, for each protocol and then for each state. This tier is intuitive for the user, but easily overridden.

Supported Protocols

Protocols will be defined, in collaboration with the industry experts by way of membership bodies. For each communication type, the protocol will be defined and versioned for implementation in applications and devices. Certain protocols are easy to implement whereas others may take time. However, users and control over their preferences will drive the market and so commercial competition will drive its adoption.

The protocol will be designed for speed and ease of use. In addition, underlying implementations will be developed to gain the widest vendor uptake by standardising on recognised unconstrained(RESTFUL) and constrained(CoAP) transport protocols:

Non-constrained devices / applications
RESTFUL - https://www.w3.org/2001/sw/wiki/REST

Constrained devices / applications
CoAP - https://tools.ietf.org/search/rfc7252

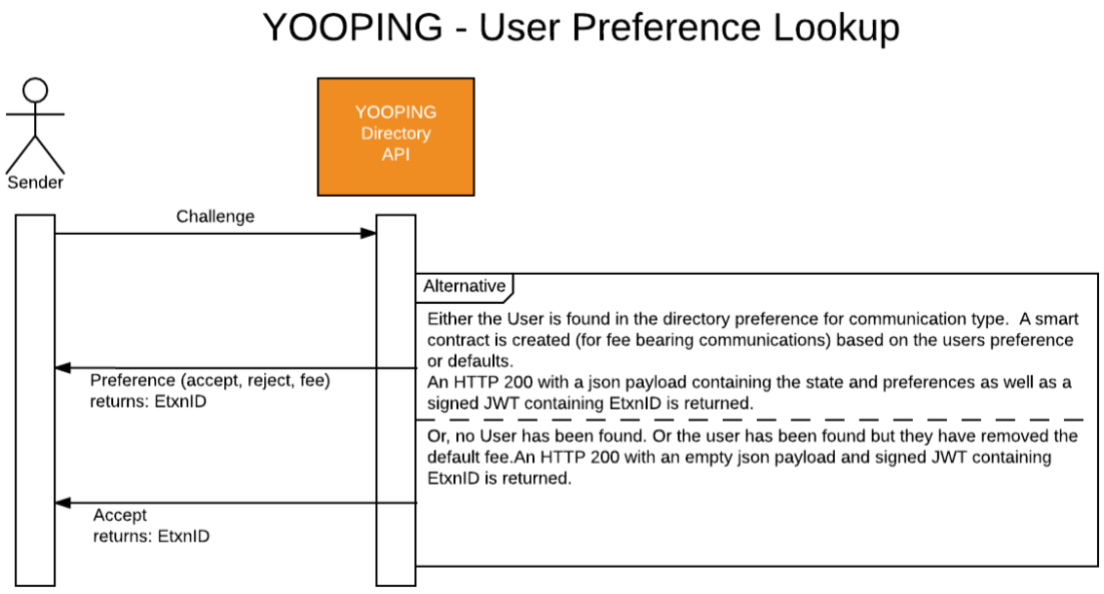
The Challenge Phase

The challenge phase allows a sender to make a fast enquiry for the recipient's preferences. The challenge phase will allow the sender to establish the communication or query the sender before doing so. The response to the challenge protocol will contain the user's preference, their language, any fee and currency and a JWT which will be passed to the recipient should the communication proceed.

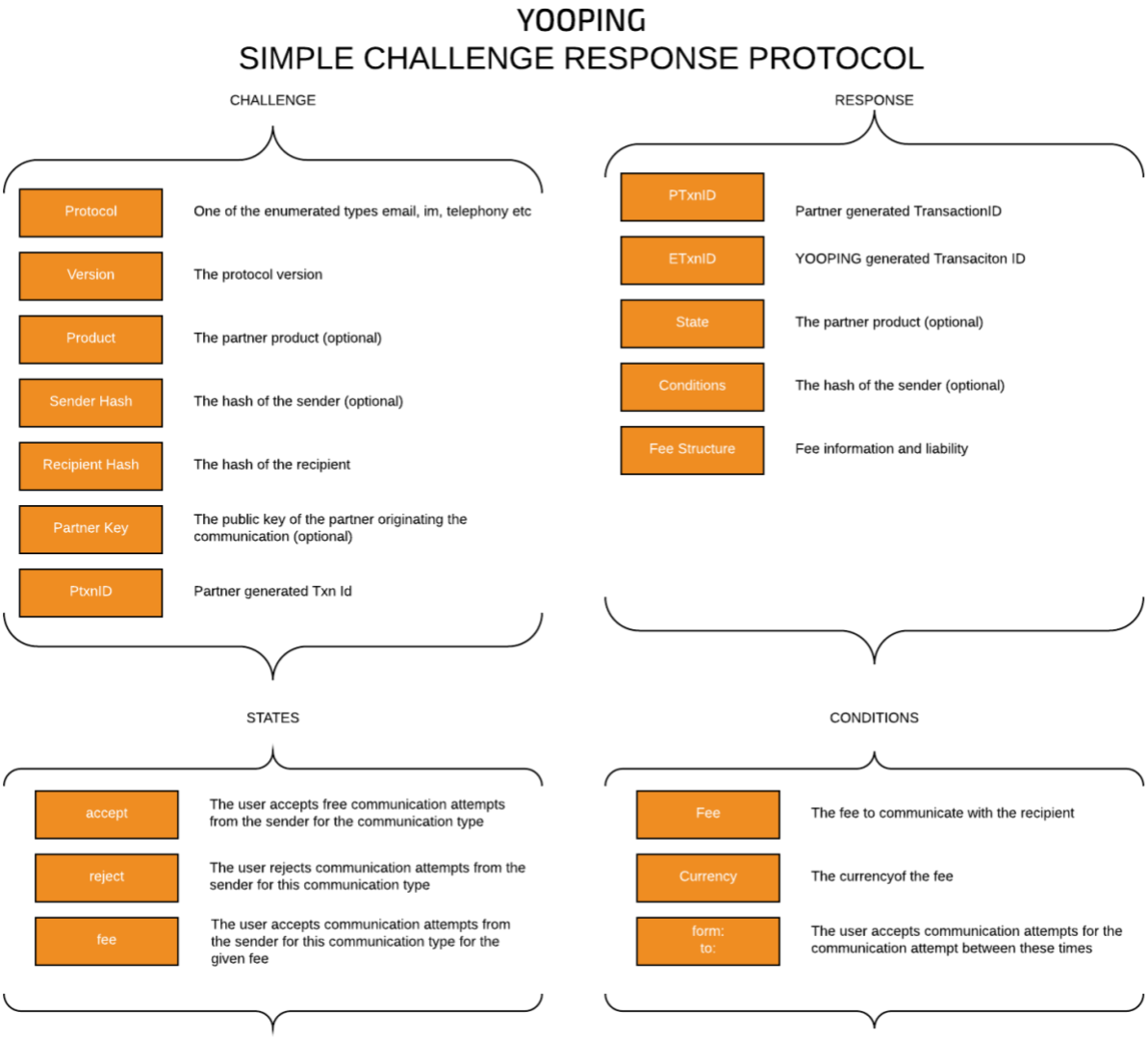
The JWT allows the recipient to authenticate the validity of the request without a subsequent network call and contains a "Time to Live" to ensure the communication is timely.

If the challenge phase determines the recipient allows communication, it proceeds.
If the challenge phase determines the recipient does not allow communication, it should not proceed, as doing so will be rejected and a smart contract will have applied a financial penalty.
If the challenge phase determines a fee is involved, the sender application must solicit a decision from the user, informing them of the financial cost of the transaction. The communication will be sent, but there is no guarantee what the recipient will do with it.

In case of instances, such as telephony where communication is established, but a voicemail service may prevent communication, a duration of 10 seconds allows the sender to decide if they want to proceed with the communication or not. The smart contract can then be cancelled within this time by the sender making another call to the platform.



Challenge Protocol



The challenge phase uses a standard HTTPS post request (uses TLS Transport Layer Security) to send details to the API. The YOOPING platform authenticates and derives the appropriate response using the user's preferences and responds with a json payload and JWT.

In the background, any fee payable is created in advance (which ensures the financial commitment is created prior to sending the communication) using smart contracts whilst obfuscating the sender and recipient. The contract will then handle billing and apportion credit to the entities based on the revenue model and sender decision. The result of the smart contract is determined by the sender's decision, based on the user's preference.

The Initial Communication

The sender delivers a communication to the recipient. Even if the recipient accepts this (and subsequent communication) a small fee is levied to produce revenue for the platform.

An Accepted Communication

The sender delivers the communication to the recipient, because they have stated in their preferences to accept them. There is no smart contract and therefore no fee to pay.

A Rejected Communication

The sender decides to risk the fee to deliver a communication to the recipient. The recipient decides to reject this (and may also block subsequent communication from the sender) and therefore the fee is apportioned between the user, partner and platform.

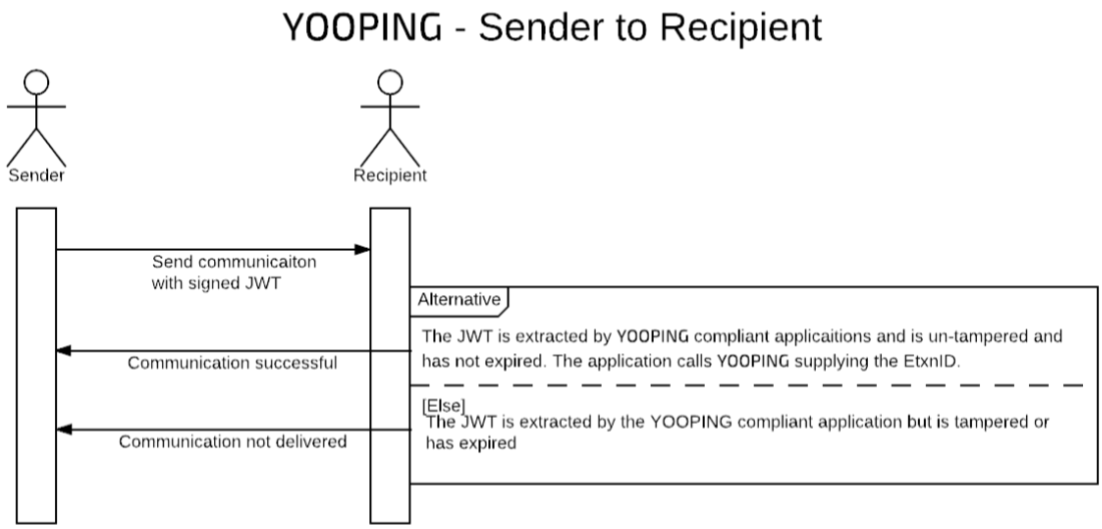
A Communication with a Fee

The sender decides to communicate with a recipient who requires a fee. The communication is delivered and the fee is apportioned between the user, partner and platform.

Integration and Legacy support

Mode 1 - “compliant sender” to “compliant receiver”

This is the desired state or the “happy path”. A YOOPING user is sending communications to another YOOPING user, where both parties are using applications that adhere to the protocol.

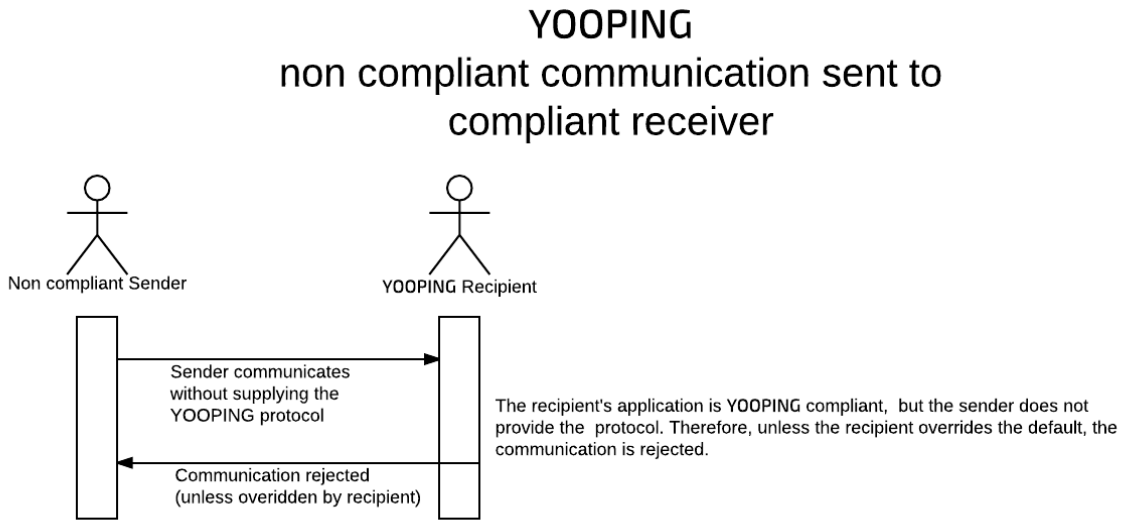


The protocol still ensures the communication is valid, has not been tampered with and has not expired and the application performs the necessary action to either deliver or reject the communication.

Depending on the Recipient's preference, the sender may have to (or may have agreed to) pay for the privilege of sending the communication, but the fee arrangement and process has happened behind the scenes, using smart contracts prior to the JWT being signed and transferred to the recipient.

Mode 2 - “non-compliant sender” to “compliant receiver”

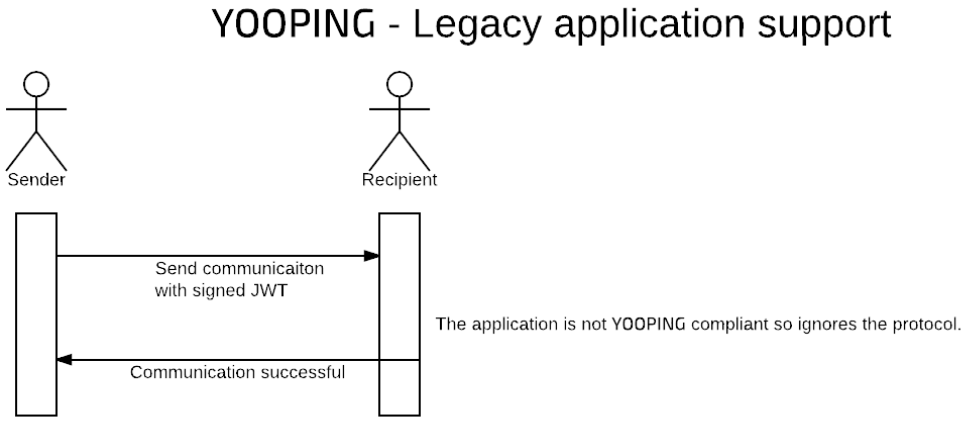
Where a recipient has decided to upgrade to an application or device that supports the YOOPING platform, they would expect communications from legacy or non-compliant applications to fail (unless they specifically allow them). The platform has been designed to support this operation.



This is the main barrier in intercepting spam emails and Phishing attacks. The default is to reject the communication unless it can be authorised from a non-repudiated source. As soon as users upgrade to YOOPING and use a compliant application or device, the default is to protect them. Therefore, vulnerable or less technically able people can be set-up and afforded immediate protection from a large source of fraud.

Mode 3 - “compliant sender” to “non-compliant receiver”

The YOOPING platform can be introduced without affecting the current communication protocols. If a user initiates a communication with another user who has not upgraded to an YOOPING compliant application or device, then they would expect the communication to succeed.



This mode allows user who have upgraded to YOOPING protection to still contact recipients who have not. The platform has been designed to provide inbound protection without compromising outbound connectivity. For example, if a loved one has not upgraded, we still need to contact them. Once they upgrade, we can add them as an ACCEPT(ed) sender and receive free communications.