Decentralised

TRUST & REPUTATION PROTOCOL

for **THE INTERNET**

The largest anti-fraud and URL reputation database is heading to the blockchain

ANTI-FRAUD

ANTI-PHISHING

ANTI-MALWARE

BRAND PROTECTION

NEWS CREDIBILITY

CHILD SAFETY

Better security for:
ISPs, WiFi Providers, Mobile Device OEMs, Apps, APIs...

TRUST & REPUTATION PROTOCOL

We see a world where you feel safe opening a link

POWERED BY

METACERT PROTOCOL

Table of Contents

DESIGN GOALS

Reputation Behavioral Signals
User Interface
Adoption Strategy
Who Will Use the Protocol?

SOLUTION: THE METACERT PROTOCOL

Decentralized Registry
Address the Identity Problem: Verified vs. Suspicious or Fake
Address the Trust Problem: Real vs. Fake
Real-time Protection Backed by Community Verification
Incentivize Community Contributions with Tokens
Freedom to Build Great Products and Services

FUTURE WORK

Nodes
Protocol Categorizer
Protocol Validator
Node Operator
Mitigation of Potential Risks

REFERENCES AND FURTHER READING

Introduction

Our Vision

We are building an open security protocol for the Internet relaying trust and reputation information about Uniform Resource Identifiers (URIs) including domain names, applications, bots, crypto wallet addresses, Application Programming Interfaces (APIs), and content classification. The Protocol's registry is machine-readable and queryable for use by Internet Service Providers (ISPs), routers, crypto exchanges, Wi-Fi hotspots, mobile devices, browsers, websites, and applications to help address cyber threats such as phishing, malware, brand protection, child safety, and news credibility.

Abstract

Not a week goes by without news of a crypto exchange being hacked [1], a major corporation or public institution suffering an Internet security breach or innocent victims falling prey to phishing scams [2]. Internet security is a critical necessity for organizations and individuals, but remains one of the most difficult problems to contain because threats continue to evolve.

MetaCert, the author of this document, isn't just a company; we are a group of individuals driven by our collective passion to protect people from personal and financial losses and give guardians the chance to protect children from inappropriate content.

The team behind MetaCert has been working for years to create and maintain standards for security across the Internet. MetaCert's founding members helped to create the W3C [3] Standard for URI[1] Categoriza-

[1] Uniform Resource Identifiers (URIs, aka URLs) are short strings that identify resources on the Internet: documents, images, downloadable files, services, electronic mailboxes, and other resources. They make resources available under a variety of naming schemes and access methods such as HTTP, FTP, and Internet mail addressable in the same simple way.

tion - the most widely used standard across the Internet. Today, the MetaCert team combines its expertise in setting URI standards with years of experience in the realm of online safety and security in order to shift one of the world's biggest cyber threat intelligence systems of URIs to the Blockchain (a distributed ledger). Therefore, MetaCert will introduce an open protocol called the MetaCert Protocol ("the Protocol") that will improve the Internet's trustworthiness and reputation.

Using distributed ledger technology, MetaCert will decentralize its categorized and currently centralized registry of URIs to democratize the submission, validation and dispute processes for URIs.

To enable the growth, development and utility of the Protocol, we are launching the META Token (the "Token"). Once the Protocol is operational, the Token will be the foundation of a Tokenized economy that incentivizes users to behave appropriately, mitigating the risk of bad actors and reducing community security vulnerabilities.

What Motivates Us

We believe in a free, open and safe Internet for everyone where the public can access the resources they want while avoiding content they prefer not to see. You should feel confident identifying and avoiding dangerous links and be empowered to safeguard yourself and your children from links with inappropriate or distasteful content.

We believe it should be easy for people to avoid phishing scams, malicious software (malware), and other fraudulent, intrusive, and deceptive ploys.

We believe it should be easier to tell the difference between what is real and what is fake news, so society can make better informed choices about who they vote for. And we believe brands should be protected so their consumers don't become victims of online fraud.

These are just some of challenges we have been working to address for the past seven years.

The Problem

Who is the real owner of example.com? Is this app safe to download? Does this website contain JavaScript that will hijack my computing resources for crypto mining [4]? Is this content safe for kids? Does this news article come from a reliable source? Has this crypto wallet address been verified? Is this a fake Twitter account?

Each of these questions implicates an important aspect of the Internet -- Uniform Resource Identifiers (URIs). URIs are used to identify resources such as domain names, social media accounts, news articles, apps, bots, crypto wallet addresses, APIs, or IoT devices, but can you rely on the safety of a URI before opening it?

The general issue with trust and reputation on the Internet is a question of checks and balances: who checks the checkers and who decides who can be trusted? Until now, users have had little choice but to trust centralized organizations with an almost monopolistic grip on what is considered trusted.

Even open source, transparent lists are just arbitrary lists of URIs that are considered good or bad. Where's the guarantee each item on these lists is error free and genuine and if users rely on them, where's the guarantee they will remain up-to-date?

What about Extended Validation (EV) certificates? These types of certificates require a more rigorous vetting process for verifying ownership of a domain, confirming the physical location and the asserted identity of the legal entity requesting this form of certificate. Despite good intentions, recent research has shown that EV certificates can be abused by bad actors [5].

In short, users don't know who to trust. Opening the wrong URI can result in users logging into a phishing website, having their personal information stolen, or losing their cryptocurrency. Users may also end up downloading malicious software (malware) or ransomware onto their devices.

We believe the problem can be distilled into three main issues:

1. Users are not adequately capable of detecting and avoiding security threats due to ineffective threat identification and categorization

2. Detected threats are often incorrectly categorized

3. Users and service providers aren't properly incentivized to fix the existing detection and categorization issues

The Proposed Solution

Over the years, MetaCert has researched and developed one of the world's most advanced crawlers and threat intelligence systems for categorizing URIs. Using our proprietary technology, innovative approach, and help from thousands of people in our community, we have built one of the biggest sources of trust and reputation information about URIs in the world.

MetaCert is building a query and response protocol on the blockchain that stores open sourced and community verified information on resources such as domain names, IP addresses, social media accounts, bots, applications, crypto wallet addresses, or autonomous system identities. The Protocol stores and delivers content in a human and machine readable format. The information stored on the Protocol can be used by anyone to build products or services to address issues such as phishing, malware, brand protection, child safety, and news credibility.

Using the blockchain, it is now possible to create new open systems that curate data sets through smart contract rewards, incentivize good behavior and mitigate the risk of bad behavior using fairly applied counter-measures and punishments. Once structured and populated on the main blockchain or its side chains, these curated data sets become immediately eligible for global distribution on a mass scale.

The Protocol is a special case of this incentivized curation and distribution network, extolling security, openness, and transparency across the entirety of its operations. The Protocol will contain the world's foremost

high-quality information and determinations on URI reputation and it cannot be edited without an audit trail for all to see.

With the Protocol, the trust and reputation of the Internet is placed back into the hands of everyday people. It will be enabled through a system of checks and balances to ensure high quality participation and authentic behavior that is incentivized by a Tokenized economy.

The MetaCert Protocol

The Protocol will be accessible to any user anywhere in the world. All these users will need is access to a computer or smartphone to submit, review and validate information about URIs. This user reporting will then be permanently stored in the Protocol.

Through the Protocol, behavior that results in higher quality URI reputations will be rewarded while behavior that subverts or undermines integrity will be punished. At the core of this is an incentive system backed by the Token, which may be staked to “claim” and validate the membership of a URI to a specific category and be further applied as tender for access.

Participants

Participants are generally passionate about a particular subject matter. For instance, crypto enthusiasts are keen to avoid online fraud and phishing scams that can lead to the theft of their crypto assets, or guardians using parental controls to prevent kids from accessing adult content on the Internet. These users are incentivized to report suspicious links so the security tools they use for protection are improved by their participation. Some people are simply passionate about helping to make the Internet safer for everyone.

While we anticipate that new classes of participants will emerge as dictated by the evolving practices, dynamics and needs of the community, we have identified at least four primary classes of participants that will interact with the Protocol, namely Submitters, Validators, Purchasers and End Users.

Submitters

Submitters are a class of participants that identify URIs that have yet to be categorized by the Protocol, or require updated classification information. They are able to use a web interface or mobile app to submit information about URIs, which is then placed into a queue for validation. This information could include classification of a domain, ownership of a domain, its contact information and more.

Resource owners are a unique example of Submitters who also play an important role in the Protocol. Unlike other Submitters, resource owners initiate the validation process for their domains, crypto wallet addresses, social media accounts, and other internet resources by paying Tokens. The validation process is in turn funded by the Tokens resource owners pay, helping to form the backbone of the Protocol's economic engine. Once a submission from a resource owner is approved, they will be notified, and the validation process will commence.

Validators

Validators are a class of participants responsible for reviewing URI submissions before they are added to the Protocol. They are awarded the "Validator" status if they attain a high quality of accuracy, determined from repeated successful reviews pertaining to the categorization of these respective submissions. They can also achieve this if they're considered "experts" for a respective category, for example an "anti-phishing" expert with 10 years professional experience.

Purchasers

Purchasers are a class of participants that purchase access to the Protocol for integration into their own products or services. Purchasers have the ability to pay for access to the entire Protocol, multiple categories or a single classification type. Access can be obtained by making a payment for monthly access or annual access, which includes a discount.

End Users

End Users are a class of participants that are the primary beneficiaries from the availability of the Protocol. These include users of products like Cryptonite, the MetaCert Telegram Security Bot, the MetaCert Slack app, or future products that have yet to be created by developers, companies or any other type of Purchaser.

Protocol Incentives

Knowing the roles of the participants in the Protocol serves as a starting point to understand the value of the incentives in this system. There are several highlights of this incentive system including:

- URI Submitters and Validators can lay claim to a certain number of URIs. These claims allow Submitters and Validators to collect fees on access to the respective URIs as they are accessed by Purchasers. The amount of allowed URI claims depend on the amount of staked Tokens. This limit incentivizes Submitters and Validators to claim the most useful and accessed URIs.

- Early Submitters and Validators for a specific URI category will earn a disproportionate interest in the fees collected for data access. Early confirmations are typically more valuable than subsequent confirmations.

- Submissions and validations may expire or depreciate their owners' fee interest over time or upon some event, as stale data become less valuable. This creates a new incentive for Protocol participants to re-submit and re-validate existing URIs that may have become outdated.

- Stakes can be slashed, such as if the network disagrees with a Submitter or Validator, and all decisions are immutably logged to the ledger for review and identification of bad actors.

- Participants may pay in Tokens, fiat, or other cryptocurrencies for access. As part of its technology adoption strategy, MetaCert may issue accounts and browser extensions with pre-credited access to the network data.

Reputation Score

Participants in the network are each given a reputation score, which is comprised of various behavior signals derived from their participation in the Protocol, including their track record in submitting and validating URIs, level of recorded expertise, and other data points that are defined by the system.

Tokens will be distributed to incentivize participants to tell the truth when submitting or validating URIs recorded on the Protocol. However, the history of crowdsourcing has demonstrated that it is impossible to rely on good faith alone, so we use software and incentives to help identify trustworthy or unreliable participants and their associated reputation score.

The reputation score will also contribute towards activity within the system. For example, phishing-related submissions from an anti-phishing expert will be more quickly validated and such an expert may also act as a Validator for phishing submissions from non-experts. However, an anti-phishing expert doesn't have much experience identifying credible news sources, so their news submissions require more validation work and they may be unlikely to become a Validator for news submissions.

Token Mechanics

Staking for URI Claims

Submitters and Validators stake the Token to claim submissions and validations of a URI belonging in a certain category. The number of URIs that a staking amount can claim varies depending on parameters such as the category, link query traffic, and possibly metrics related to reputation. Staked Tokens can be challenged and lost if submissions and validations are overturned.

The stakers may earn future revenues on the claimed URIs by successfully identifying, submitting or validating the URIs. They are also entitled to a portion of the URI query fees paid to access the information that they discover. Stakers can only earn revenues based on their own directed efforts and the market's demand for those efforts. The fee amount will depend on a number of factors such as the importance of the submissions and validations, time-value of information, and ease of validation. Information about URIs become stale over time and so should the amount of fees collected by purveyors of older information compared to newer information. Additionally, the network collects a marginal fee to sustain its perpetuation and for improvements, but does not seek to earn a profit.

Because a Submitter or Validator can claim a limited number of URIs proportional to their staked amount, the time-value of money creates an economic incentive to pick the best, highest trafficked links for submission and validation. This serves to ensure data quality on the network and prevent market congestion in which URI submissions are brute-forced and the network becomes relatively useless. The primary determinant is the size of the participant's stake, the amount of effort expended by the participant, and the selection of the categories and URIs on which to expend these efforts.

Validation Fees

Tokens are rewarded on a sliding scale based on the complexity and importance of the information being submitted and validated. For URIs that are more difficult and time consuming to identify, review and validate, such as a phishing website, users will earn more Tokens. Similarly, time consuming verification efforts such as verifying ownership of a resource like a domain name, bot, app, or API will be rewarded with a greater amount of Tokens.

Owners of resources will have the option to place Token bounty incentives so that Submitters and Validators are rewarded for their participation. This creates a signalling mechanism in which URI owners may request the scrutiny of the network's Validators for certain relevant checks. Diverse validations across ownership, domain names, and site content will start scarce and become comprehensive over time, possibly supplanting Extended Validation certificates in both usefulfuness and trustworthiness while extending verification beyond domain name ownership.

In the future, the number of Tokens awarded to participants will be determined by the utility of the category. For example, a URI that is categorized as sports may earn each participant less than a phishing submission due to phishing being more difficult and time consuming to detect compared to sports content. Phishing also requires anti-phishing experts to validate submissions whereas URI submissions for sports wouldn't require an expert in sports to validate it. It may require multiple people who meet a combined reputation score where their category experience isn't a prerequisite.

URIs that require validation will be randomly divided amongst all validating participants to prevent coordinated groups from carrying out centralized voting bias. Furthermore, Submitters and Validators will start with a low reputation score, allowing them to participate with a small number of submissions and validations. As their reputation score increases, the number of URIs they can submit or validate in a given timeframe will increase. For example, new participants will be restricted to 5 URIs per day.

Improved Brand Verification Process

We are designing a new and improved verification process for registered users or assignees of Internet resources, such as a domain names, IP addresses, bots, applications, crypto wallet addresses, and social media accounts. This will help protect brands on the Internet from impersonators damaging their brand. We believe this new verification process can be more economical, transparent, and accessible for any user and also address the challenges of Extended Validation certificates. Brands will pay in Tokens to submit their domain names and social media accounts to be verified. Protocol participants will then verify the integrity of this information. Once a brand's submissions have been verified as true, the information will be stored on the blockchain.

How Tokens Can Be Used

The following are a few example use cases demonstrating how Tokens are earned and spent by participants in the Protocol.

EXAMPLE:

Paying for Services Utilizing the Protocol

The most natural use case for the Tokens is the ability for individuals and companies to use them to pay for a variety of security products and services that incorporate the Protocol. Existing products offered by MetaCert will be the first to utilize the Tokens as a payment method with other companies looking to do the same for their own integrations. In addition to paying for products and services, users will be in a unique position to earn Tokens by submitting and validating URIs on the Protocol. Their participation not only serves as a way to help protect themselves as well as others, but also gives them an opportunity to earn and spend Tokens for these products.

EXAMPLE:

Community-Driven Child Protection

Jackie has two children, Adrian age 7 and Sophia age 12, so she uses

parental control software to prevent them from stumbling upon adult content on the Internet. Jackie is also an active participant in our network and submits and validates adult content that her children might inadvertently access. For her efforts, Jackie is rewarded in Tokens which may be used to pay for the parental control software that protects her children or sold to other parents who might wish to pay for the same software themselves.

EXAMPLE:

Payment For Validation By Resource Owners

An individual, group, or company owns Internet resources. They turn to our verification platform to ensure users are not lead astray when attempting to access these legitimate resources. To fund the validation on the Protocol, resource owners pay Tokens. In turn, Validators who participate in verifying that resource are rewarded with a share from the owner's Token payment.

MetaCert's Prior & Related Work

Crawlers and URI Categorization Technology

MetaCert built one of the most advanced Internet crawlers and URI categorization technologies in the world after realizing that every filtering tool on the market used antiquated techniques and technology, resulting in ineffective classification with high volumes of false positives. Existing systems built on legacy architecture failed to address the changing needs of today's users. Over the past seven years, the MetaCert crawler gathered, categorized, and indexed over 10 billion URIs across 65 categories.

MetaCert is the only company in the world today capable of categorizing any part of a URI. For example, consider how http://imgur.com/r/nsfw would be categorized using MetaCert versus other existing technologies. Using MetaCert's proprietary technology, imgur.com is categorized as "Image Sharing", and /nsfw/ is categorized as "Pornography." This level of granularity is a major advantage that MetaCert has over existing technologies.

This means the Protocol will be the very first that will allow people to submit and validate information about resources such as social media accounts and folders with user generated content without having to submit and validate the entire domain name. This includes resources that go undetected by many cyber security companies like OpenDNS [6], Symantec [7], Bluecoat [8], and which evade detection by the Google Safe Browsing API [9].

To put things into perspective, OpenDNS, one of the world's most respected filtering companies, receives over 135 billion DNS requests

daily and has categorized 2 million unique domains into 65 categories. In comparison, MetaCert has categorized over 7 million unique domains just for Pornography, which is just one of over 60 categories.

We have over 800,000 unique domains in our review queue. These domains will be moved to the blockchain, where anyone will be able to sign-up to review and validate them in return for Tokens. By combining our existing wealth of data, designing a system to manage the integrity of this and all future data stored on the blockchain through a Tokenized economy, we are laying the foundation for the Protocol described in this paper.

Our fully functional existing products will benefit from the transition to use the Protocol.

A Proven Track Record In Crypto

We have an established suite of security products that use the centralized categorized registry discussed throughout this document. Each product showcases how each of the security categories can be utilized.

MetaCert Security Slack Bot

MetaCert is one of the most established security companies in the messaging space. SingularDTV [10], a Blockchain Entertainment Studio, reached out to us for help in 2017 to protect their Slack community. Since then, MetaCert has become one of the most trusted companies when it comes to protecting Crypto companies such as Mercury Protocol [11], BigchainDB [12], Neufund [13] and COSS [14] from phishing scams inside their Slack communities. Our software, the MetaCert Security Slack Bot [15] currently protects over 250,000 people, and continues to grow.

MetaCert Security Bot for Telegram

Messaging service Telegram, which boasts over 200 million monthly active users, has become a prominent choice for hosting crypto communities including MetaCert. As these communities flourish, they've become ripe for phishing scams.

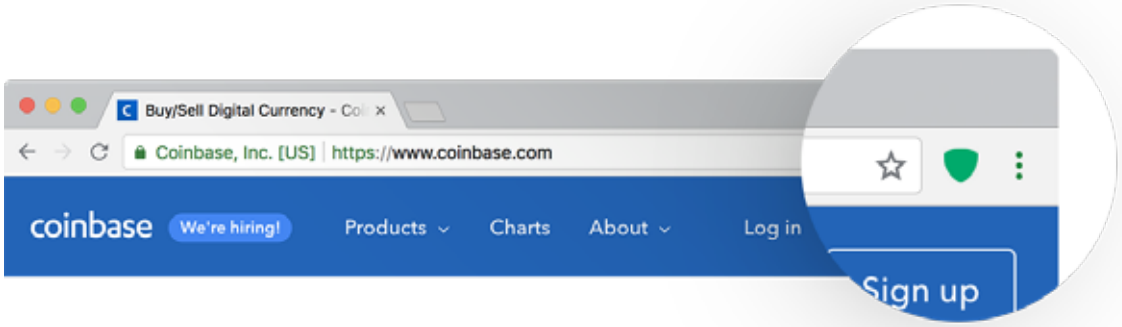
We launched a Security Bot for Telegram [16] in March 2018 to address these issues and the community responded favorably. This Security Bot currently protects more than 350,000 crypto enthusiasts across a number of communities and its adoption continues to grow.

Cryptonite Browser Extension

In December 2017, MetaCert started a social experiment to see if it was possible to build an entirely different solution for domain ownership verification — a process that could reduce the risk of phishing by more than 95%. We built and published a browser extension called Cryptonite [17] for Google Chrome, Mozilla Firefox and Opera Browser that verifies domains owned by cryptocurrency exchanges, projects, and wallets.

The screenshot above shows a Crypto company educating their community to look for the Cryptonite shield when visiting their website.

When an End User visits a site that is “Verified by MetaCert” like Coinbase [18], Cryptonite changes the color of the Cryptonite shield on the browser bar from black to green, thereby indicating they are on the real Coinbase website and not a new phishing domain that hasn’t been discovered yet.



The feedback on this product has been overwhelming. Cryptonite gained over 50,000 active users in the first six weeks of launch. Users want to remain safe when buying and selling crypto and our user base continues to grow.

We now receive requests from some of the biggest exchanges in their respective jurisdictions, from Sweden to Malaysia, to verify their domains as their communities are complaining about not being verified by MetaCert.

Active Participation In Community Growth

A number of our customers and their End Users are consumers and contributors to our existing centralized, categorized registry. Many of them submit and validate URIs already and this existing network of participants will help accelerate the growth of the Tokenized economy for the Protocol.

We currently maintain products using our registry in the following categories:

- Phishing
- Malware
- Child Safety
- Brand Protection
- News Credibility

In addition to providing products utilizing the Protocol, we want to see the development of new and innovative applications of the Protocol that haven't yet been considered. To facilitate this, we will provide Token grants and incubation to help third parties build new products and services that address real, everyday problems on the Internet.

A Team With Proven Domain Expertise and Experience

Paul Walsh, our founder and CEO, co-initiated the creation of the W3C[2] Standard for URI Categorization that formally replaced Platform for Internet Content Selection (“PICS”) [19], the previously used worldwide standard in 2009.

Paul also holds a U.S. Patent for in-app WebView security for anti-phishing based on the URI categorization with two more patents pending for advertising, news credibility, and many other categories.

Ian Hayward, our COO, sponsored the engineering build and maintenance of spreadfirefox.com [20] as Mozilla’s lead community admin from 2005 to 2009, where he helped guide Firefox’s grassroots community marketing. It is Ian’s unique approach to open source projects that enables MetaCert to build and support an active contributor and evangelist community.

Overcoming the Challenge of Crowdsourced Data

While crowdsourcing does exist for some URI categories, it only covers a fraction of potential threats on the Internet and it doesn’t properly incentivize participants. This is because centralized entities are more concerned with “owning” trust and reputation than they are about building a more secure network.

PhishTank [21], launched in October 2006 as an offshoot of OpenDNS (Cisco), offers a community-based phishing verification system where users submit suspected phishing websites and other users "vote” on whether it is a phishing website or not. Unfortunately, because contributors don’t get rewarded for their participation and it is relatively easy for bad actors to spoil the quality of this data.

[2] The World Wide Web Consortium (W3C) is the main international standards organization for the World Wide Web.

By moving their efforts from PhishTank and other similar lists to our Protocol, contributors will be rewarded for their hard work and have a say in the future governance with the ability to react much faster to changing markets and product needs.

Historic Approaches

PICS was a specification created by W3C that used metadata to label webpages for the first time to help parents and teachers control what children and students could access on the Internet. The W3C Protocol for Web Description Resources project integrated PICS concepts with the Resource Description Framework (“RDF”).

PICS often used content labeling from the Internet Content Rating Association [22], which has been discontinued by the Family Online Safety Institute's board of directors. Internet Explorer 3, released in 1996, was one of the early web browsers to offer support for PICS. With the release of Internet Explorer 5, Microsoft added a feature called approved sites, which allowed extra sites to be added to the PICS list when it was being used. Apple’s parental controls still relies in part on PICS labels on websites today.

PICS was superseded by the Protocol for Web Description Resources (“POWDER”) [23] in December 2009, a system that was co-initiated by Paul Walsh and Phil Archer. Although MetaCert doesn’t strictly use the POWDER specification, our founder’s work to establish it demonstrates how MetaCert became the world’s authority on URI Classification and Content Labeling. Paul Walsh has been working on URI Classification and Content Labeling techniques, standards and tools since 2004 when he founded a Web Accessibility Compliance Certification company called Segala. Ian Hayward built the first browser extension for Segala, which was later formally endorsed by the W3C as one of the most compelling implementations of the semantic Web.

Design Goals

The Protocol can become the world’s biggest decentralized, categorized registry of URI intelligence with the highest quality of data. If this comes

to fruition, we expect the Protocol to be the de facto protocol layer for determining trustworthiness and reputation of URIs. The Protocol will also be designed with ease of use in mind, so participants can contribute to it through any of their connected devices and applications.

The Tokenized economy of the Protocol is being developed to scale faster than any previous or existing threat categorization methods because of its built-in incentives, and it will be infinite because it is hosted on the blockchain. The Protocol will enable participants to contribute to something that is profound, benefiting people today as well as future generations.

Our Protocol will enable anyone to submit URIs for categorization. The Token allows us to incentivize good behavior while removing the attraction for bad actors to submit poor quality data.

Individuals who are considered experts in their respective fields can quickly become Validators while others that are not classified as experts or experienced in a particular category can submit URIs on day one. They can strive to become Validators once they have achieved “expert level” reputation for categories on the Protocol.

Reputation Behavioral Signals

We are designing an incentive system whereby Submitters and Validators are each given a weighted reputation score based on behavioral signals and other data points from interaction with the Protocol.

The system is constantly attributing reputation points towards each participant’s reputation score based on the recorded outcome from each of their submissions and validations.

The following list displays how reputation points may be allocated to each participant. Some or all of these may be considered depending on the resource type being categorized and the information that is being attributed to that resource. These signals include:

- Total number of submissions
- Percentage of submissions that were validated successfully

- Percentage of submissions that were unsuccessfully categorized
- Percentage of submissions that fail to resolve (e.g., there is no content on the domain name)
- Length of time a participant has been in the Protocol
- Number of submissions associated with specific resource types or categories (e.g., if a Submitter always submits URIs to be validated in the Sports category and they are always validated, they might be flagged to become a Validator of future Sports submissions)
- The utility of submissions (e.g., if a Submitter has a low frequency of participation but the quality of their submissions is high and the utility is high due to the consumption of the data, they may be considered for becoming a Validator)

This is not an exhaustive list as the Token mechanics are far more complex in reality. While we don't yet apply Artificial Intelligence ("AI") to further improve the reputation system for our Token, we will implement machine learning techniques from the start so we can build a big enough dataset from which to apply AI in early 2019.

User Interface

MetaCert is building two user-friendly interfaces, a website and mobile app, that will allow anyone to submit, review and validate information about URIs to help categorize the Internet. These interfaces will be available within 28 days of the first Tokens being allocated to participants.

It will now be possible for anyone anywhere in the world to submit, review and validate URIs into the the most appropriate category type. All that is required to participate and be rewarded in Tokens is a computer or smartphone.

Submitters propose a category and other additional information, and Validators review and validate their submissions. Participants will be able to check their Token rewards from the website dashboard or app.

When someone submits a URI for categorization such as “Pornography,” crawlers and other tools are used to automatically validate submissions. Each URI that is not categorized is added to a review queue. Validators may access the review queue and earn Tokens by helping to validate these URIs via the web interface.

With nearly one million unique domains waiting to be reviewed, both submitters and validators will be able to review and propose a suitable category for each domain on day one – earning Tokens immediately.

Authorized add-ons such as MetaCert’s own Cryptonite or others such as the popular MetaMask [24] extension, may be used to enable submission and validation of links for registered users. These add-ons will also have the capability to store Tokens earned that users can then add to their wallets at a later date.

User interaction touch points will be created in our Slack, Telegram, Skype and Messenger bots to easily submit as well as potentially validate URIs.

Adoption Strategy

MetaCert currently has paying customers that consume and contribute to our proprietary, centralized, categorized registry. To kick-start participation in the Protocol, we will incentivize our existing community and End Users to become contributors by rewarding them for the participation they already contribute as goodwill.

The early participation of existing users to submit and validate URIs will greatly encourage future participants. This effort will help create and demonstrate best practice principles to users of other products from companies such as messaging platforms, browser vendors, and others that build upon the decentralized Protocol.

Many companies install MetaCert to protect their end-users from phishing scams inside Slack, some of which comprise of communities consisting of greater than 10,000 users. Every End User is a potential participant in our registry as their submissions and validations would improve

the registry that is used to protect them.

Many customers and End Users already report phishing links on a daily basis. We look forward to being able to reward them for their work and automating the process of validation through the Protocol, thereby removing MetaCert as a central authority in the validation process. Participants and stakeholders will use multiple channels to report these links — via email, Twitter, their own Slack community or through our own Slack group.

When a crypto company installs MetaCert for Slack, it automatically protects their public and private channels. However, users must activate the MetaCert Slack bot if they want their direct messages (DMs) protected. Given that most phishing scams are sent via DMs, it is vital that users activate this security feature. While customers do their best to encourage users to activate the bot, it remains an uphill battle to educate them.

We will reward End Users with Tokens upon their activation of MetaCert provided security feature(s) required to protect their DMs. We will also reward customers for every user who actives the bot. By rewarding each stakeholder for diligent security practices, we will end up with a better protected community and an amazing content marketing strategy for MetaCert. Customers and End Users who report suspicious links will also be rewarded with Tokens.

By getting the MetaCert brand and value of the Token in front of every community protected by our software, we increase the number of Token participants in our Protocol. MetaCert is the company Crypto companies turn to when they require advice about security or better protection for their community, and our customer base is growing.

Who Will Use the Protocol?

We envision the MetaCert Protocol as an additional layer to the Internet Protocol Stack. It can serve as an integral protocol on the Internet or it can be integrated within hardware or software that sits on top of the

Internet. The Protocol will therefore be employed by a variety of users, from those browsing the Internet with safety in mind, to developers and companies wanting to purchase access to the data in order to focus their efforts on building their products and services.

Information stored on the Protocol and accessible by Purchasers will include (i) ownership identity, (ii) reputation ratings, (iii) content category type, (iv) submission information, (v) validation records and (vi) dispute timestamps.

The Protocol will provide purchasers an opportunity to integrate the data directly into their existing products and allow innovators to create new products that would not have been possible without it.

The following are some of problems we believe the Protocol can and will address:

Web Browsers

PROBLEM: There are a variety of third party blocklists used by web browsers to help identify and block known malicious and phishing websites, including cryptojacking malware and fake cryptocurrency exchange websites. However, these lists are either controlled by a central authority or populated by members as community service without monetary reward. As such, these lists are prone to false positives and these authorities are slow to respond to new cyber threats as they rely on legacy review procedures. Additionally, these browsers do not offer a native way to block content categories, such as XXX, entertainment and others.

Security Software/Products

PROBLEM: Security companies currently provide software and hardware based products using a mix of proprietary and third party data to identify and block well known phishing, malware and ransomware websites and applications, yet these firms are not nimble enough to promptly keep up with newly discovered cyber threats.

Certificate Authorities (CA)

PROBLEM: With the introduction of free, automated certificates, there has been an uptick in the number of HTTPS phishing websites using these certificates. One particular CA has issued over 15,000 certificates for “PayPal” phishing sites. As users have been conditioned to look for the padlock, they are given a false sense of security when visiting a phishing site. In addition to free certificate abuse, industry experts are warning that Extended Validation (EV) certificates, which require a more robust verification process, can also be spoofed and used by malicious actors.

Social Networking Services

PROBLEM: On Social Networks, identity is paramount. Unfortunately, identity remains broken on these services as they are inundated by fake celebrities, influencers and brands that peddle affiliate spam and phishing websites to their users.

Web Browser Extensions/Add-Ons

PROBLEM: Existing browser security add-ons utilize centralized data, typically hosted on a few servers or vendor accounts which could be compromised. Additionally, fake versions of these add-ons are regularly installed by thousands, in some cases millions of users [25] who have few ways to verify their authenticity. Recently, Google failed to shield as many as 20 million consumers who downloaded malicious add-ons purporting to provide various services from the Chrome Web

Mobile Apps With a WebView

PROBLEM: Developers creating mobile applications that utilize WebView to display Internet content or allow users to share links have no straightforward way to block malicious content or warn users about unwanted content.

Platforms and Advertising Networks

PROBLEM: Most consumers don’t know the difference between real and fake news, and brands, agencies, and platforms don’t want to risk

their reputation by being associated with false content in their advertising. With bot armies on social networks elevating false stories, it is challenging for small, disparate teams to tackle these head on.

Crypto Exchanges and Block Explorers

PROBLEM: Currently, cryptocurrency exchanges and block explorer websites have no robust way to identify and report wallet addresses used in suspicious activity like phishing scams. Additionally, these websites do not have a way to verify known good addresses associated with Initial Coin Offerings (ICOs) or legitimate projects.

Messaging Platforms

PROBLEM: The ubiquity of messaging platforms across the Internet and mobile devices is astounding, so much so that they're largely replacing email as a preferred method of communication. As such, these platforms are hotbeds for malicious spam and phishing scams. If a messaging platform uses any third party blocklist, it is centrally controlled and isn't robust enough to react to newly discovered threats.

App Stores/ Marketplace Integration

PROBLEM: Authenticity for mobile applications in app stores and marketplaces is a problem facing End Users and developers. Over the last several months, the Google Play Store has been rife with cryptocurrency related scams [27], from fake cryptocurrency exchanges and wallets, gift offers to mobile cryptomining. These fake applications would lead to monetary loss for End Users and tarnish a company's image while cryptomining could damage one's device [28]. Trying to keep up with fake applications is challenging enough for a central authority, verifying legitimate applications is an ongoing process and it's unclear how long verification takes. This leaves a window of opportunity for scammers to take advantage of users.

Bot Verification

PROBLEM: With the rise of messaging applications and the subsequent development of chatbots, users and developers face similar chal-

lenges as mobile applications. Companies that utilize these bots give away much of their privacy. It is unclear how their information may be used in the future. Unverified bots could also be used to trick users into downloading malware or lead to phishing websites.

SOLUTION:

The MetaCert Protocol

The problems outlined above have similar challenges, which we believe can be addressed through the integration of the Protocol as follows:

Decentralized Registry

A decentralized registry of Uniform Resource Identifiers (URIs) on the blockchain eliminates the single point of failure that a central authority presents while tackling the disparate blocklists already in use by many products and services. Everyone will have access to the best and most current set of data.

Address the Identity Problem: Verified vs. Suspicious or Fake

The Protocol will help tackle one of the most common problems across many industries: identity. The decentralized registry already has a variety of information on verified and suspicious or fake resources on social networking services, mobile applications, bots in app stores and marketplaces, cryptocurrency wallet addresses, crypto exchange websites and more. Our Cryptonite browser is a great example of what developers and companies can achieve using the Protocol. There is great value in providing visual indicators to End Users, such as a green check mark or red warning page.

Address the Trust Problem: Real vs. Fake

In addition to identity, the Protocol will also be able to address a growing challenge on today's Internet: trust. Participants such as fact checking organizations and trusted Validators will help populate news into different categories. This information will be accessible to interested parties who wish to present real news and warn of fake news

while also enabling advertisers to prevent their ads from being placed with fake or undesirable content.

Real-time Protection Backed by Community Verification

Harnessing the power of the community, the Protocol's registry will contain the most up-to-date information on URIs governed by its users. Central authorities rely on proprietary data and are limited to the staff they devote to maintaining their data, which can lead to missed detections that expose their customers to cyber threats.

Incentivize Community Contributions with Tokens

Active participation in the Protocol will be incentivized by the rewarding of Tokens. This addresses the issue of existing community contributors that do so in their spare time. By offering a Token reward, not only will we be incentivizing participants to contribute, it will also ensure that they behave appropriately while mitigating the risk, incidence, and effectiveness of bad actors.

Freedom To Build Great Products and Services

Developers and companies won't need to worry about finding which blocklists to integrate with or spend time and money on developing their own. They can focus their efforts on building User Interfaces (UI) and User Experience (UX) while tapping into the Protocol and its robust community.

These are just a some of the possible problems and solutions we envision will be addressed by the Protocol. We believe our move to the blockchain will enable innovators to come up with new and useful products and we are excited to see what they come up with.

Future Work

Our system will be able to detect the utility of a submission based on how valuable it is to the Protocol. This value is derived from the usage

statistics for that URI. For example, if a Submitter has successfully helped to categorize a URI that is being blocked by one or more products that help to protect a lot of End Users, the Submitter's participation could be considered high quality.

Imagine a future where Crypto exchanges rely on a curated list of wallet addresses that contain trust and reputation information about their owners and historical transactions, or App and Bot marketplaces utilizing curated lists to protect people from fake applications that are malicious.

A particularly powerful and unique aspect of the context of this white paper is that MetaCert currently has a variety of companies and communities successfully utilizing a number of productized implementations built on top of our centralized, categorized registry.

The decentralization of this registry on the blockchain, powered by our Token means that we then have two areas to work on: (1) the production and maintenance of the MetaCert Protocol and additional spoke systems to power user interaction, i.e. validation, participant reputation, data microservices and (2) building new and improving existing products on the Protocol, e.g., products using registry categories that MetaCert specializes in.

With this in mind, when we consider future work we can talk equally about work that MetaCert can perform from a product implementation context to further the Protocol itself.

For example, future work on Protocol implementation for a category would include working with browser companies to integrate and expand the successful Cryptonite codebase. The intention would be to allow browsers to interact directly with the Protocol to provide better trust validation instead of relying on SSL extended validation certificates. We could also extend the Protocol's registry of validated wallet address for consumption via Software Development Kits (SDKs) or microservices.

Another example of future work on the Protocol would be improving

reputation management, expanding Node Operator capabilities and enhancing capabilities of category owner management.

In addition to the existing features of the Protocol, the following key areas are examples of some of the future work that we'll be undertaking as part of producing the Protocol.

Nodes

Organizations with specific expertise will be invited to participate in our Protocol as Nodes. For example, trusted fact checking organizations could become Nodes of News Credibility, being rewarded for the hard work that they already do on a daily basis.

Existing open source projects may wish to become Nodes. In doing so, they could benefit from the Tokenized reputation system while earning Tokens themselves. At the same time, they would reduce their technical support overhead — all of this while retaining control of their own branded version of the Node.

Node Operator

Node Operators are entities with computer servers that wish to host the MetaCert Protocol in pieces (Thin Nodes) or in its entirety (Full Nodes). They collect a fee for providing the data storage, computational power, and bandwidth to service purchasers of the MetaCert ecosystem.

Protocol Categorizer

Categorizers build the supply-side of the Protocol for whatever purposes they desire. A Categorizer can be individuals, groups, or companies, like MetaCert operating multiple security based categories such as XXX, phishing, and malware.

Categorizers will pay a high submission fee to create categories for resources where a guarantee of trust and reputation adds value to the demand side of the Protocol. For example, there could be categories to validate “funded startups that are hiring” where potential Categorizers

may be companies like LinkedIn or AngelList.

The Categorizer will set the percentage revenue share for Submitters and Validators within a category.

Mitigation of Potential Risks

Amongst the normal risks associated with building new things that have potential to change the way the world works for the better, some of the specific risks we are giving a great deal of consideration include the following:

> ***"How can we ensure no one single entity can dominate a category on the MetaCert Protocol that can adversely affect the quality of trust and reputation within a category?"***

We will introduce inherently designed game mechanics into the Protocol that will ensure that the owner of any category can not perform the majority of the validations of the URIs within their category. Our Protocol is already designed to reward the category owner, Submitter, and Validator where the category owner sets the percentage revenue share received by the Submitter and Validator. This means that economic market forces will determine which category gets the most participation from Submitters, who are the lifeblood of the economy.

In some cases a large entity may dominate a category, such as ourselves at MetaCert, within both the XXX and Phishing categories. In those instances where a bulk of submissions comes from a sole entity in any category they own, we will ensure a requirement for a majority of submissions and validations to come from independent parties. This restriction will provide a great opportunity for other parties to get involved in the validation processes, thereby participating in Token generation remuneration as the resources they validate are increasingly used within the market.

> ***"How can we prevent fake entries on the MetaCert Protocol?"***

The system design includes a transparent challenger mechanism that will enable anyone to dispute any entry on the Protocol. Each successful challenge of an entry will result in the relevant Submitter and Validator losing reputation value and Tokens. Exceptions to this include ownership changes, or a hacked or compromised website which has no connection to the original classification and validation.

References and Further Reading

1. CNN Tech, "Large scale hacks are among the biggest risks faced today by the global crypto community," , http://money.cnn.com/2018/01/29/technology/coincheck-cryptocurrency-exchange-hack-japan/index.html, 2018.

2. D. Mihov, “Hackers breached BeeToken’s email list and stole $1M worth of Ethereum”, https://thenextweb.com/hardfork/2018/02/01/beeto-ken-ico-hacked-airbnb/, 2018

3. https://www.w3.org/

4. D. Goodin, “Now even YouTube serves ads with CPU-draining cryptocurrency miners”, https://arstechnica.com/information-technology/2018/01/now-even-youtube-serves-ads-with-cpu-draining-cryptocurrency-miners/, 2018.

5. C. Cimpanu, “Extended Validation (EV) Certificates Abused to Create Insanely Believable Phishing Sites,” https://www.bleepingcomputer.com/news/security/extended-validation-ev-certificates-abused-to-create-insanely-believable-phishing-sites, 2017.

6. https://www.opendns.com

7. https://www.symantec.com

8. https://www.symantec.com/theme/blue-coat-acquisition

9. https://developers.google.com/safe-browsing

10. https://singulardtv.com/

11. https://www.mercuryprotocol.com

12. https://www.bigchaindb.com

13. https://neufund.org

14. https://coss.io/

15. https://metacertprotocol.com/slack

16. https://metacertprotocol.com/telegram-bot

17. https://metacertprotocol.com/cryptonite

18. https://coinbase.com

19. https://www.w3.org/PICS

20. https://wiki.mozilla.org/Spreadfirefox

21. https://phishtank.com

22. https://www.fosi.org/icra

23. https://www.w3.org/TR/powder-dr

24. https://metamask.io

25. T. Hardwick, “Fake Chrome Web Browser Extension Unwittingly Installed by 37,000 Users,” https://www.macrumors.com/2017/10/10/-fake-chrome-extension-google-web-store, 2017

26. L. Tung, “Google cuts fake ad blockers from Chrome Store: Were you among 20 million fooled?”, https://www.zdnet.com/article/google-cuts-fake-ad-blockers-from-chrome-store-were-you-among-20-million-fooled/, 2018

27. L. Stefanko, “Cryptocurrency scams on Android: do you know what to watch out for?,” https://www.welivesecurity.com/2018/02/28/cryptocurrency-scams-android, 2018

28. D. Goodin, “Currency-mining Android malware is so aggressive it can physically harm phones,” https://arstechnica.com/information-technology/2017/12/currency-mining-android-malware-is-so-aggressive-it-can-physically-harm-phones, 2017