International Journal of Academic Information Systems Research (IJAISR)
ISSN: 2643-9026
Vol. 6 Issue 11, November - 2022, Pages: 11-18

Consortium Blockchain-based Whitelisting against Quick Response Code Phishing **(QRishing)**

Hisham Sameeh Ahmed

Institute of Graduate Studies and Research
Information Technology Department
Alexandria University
Alexandria, Egypt
Hisham_sameeh@yahoo.com

Abstract - QRishing is an extension of phishing that utilizes Quick Response **(QR)** codes by encoding a Uniform Resource Locator **(URL)** of a malicious webpage/website into it, aiming to direct the user to that site. QRishing is a very dangerous and potentially devastating attack that can be combined easily with other techniques. Non-technical approaches exist that are necessary but not sufficient without reliance on technical solutions. Blacklisting is the most popular and used anti-phishing technique, however, has many shortcomings, suffers from high false positive rates and importantly subject to obfuscation and evasion techniques. In this paper we introduce a Proof of Concept **(POC)** of consortium Blockchain-based Whitelisting solution wherein, the very nature of exact match of a URL makes it almost impossible to be evaded, which is unlike Blacklisting. Every URL (long/short, static/dynamic) is an asset recorded by its owner for building this whitelist. Varied business owners will benefit to defend their assets of URLs from Banks to Coffee shops, etc., who make QR-code Ads so any real-world user can check that URLs' legitimacy. The Consortium's legal agreements, obligations and fines for wellbeing and trustworthiness is out-scope of the writing.

Keywords—Consortium, Blockchain, Quick Response Code, QR, Phishing, QRishing, Blacklist, Whitelist, Hyperledger Fabric, Obfuscation, Evasion, URL

1. INTRODUCTION

From the multiple phishing definitions listed in Computer Security Resource Center **(CSRC) [1]**, it is defined as: A digital form of social engineering that aim to trick/lure individuals into divulging/disclosing sensitive information, that the attacker will use later on for own benefits.

QR code Phishing and now QRishing is an extension of phishing that utilizes QR codes **[2]** by encoding a URL of a malicious webpage/website into it, aiming to direct the user to that site. QR codes uses has witnessed a wide variety of general use cases, in one hand; due to their fast readability feature, relatively large saving capacity to be an offline database, and in the other hand; due to the increase use of mobile devices. However, this come with risks that made a QR code an ideal method for phishing attacks due to many factors, for example: Online free-QR code generators are available, so QR codes can easily be created, printed or distributed online. Some QR code readers perform the necessary action without first getting users' approval **[3]**. The URLs decoded may be too long or understandable by humans to judge the legitimacy of such URLs **[3, 4]**, or the user may follow a link just for curiosity. In addition to, the nature of on-the-go user's interaction that distracts many users' attention from distinguishing what is legitimate and malicious to click-and-follow. Furthermore, attackers are increasingly targeting mobiles devices because the limitation of their form factor, relatively relaxed security features than laptops and desktops.

To exploit QR codes there are two main attack vectors as in **[4]**: a) The attacker/scammer replaces the entire QR code, by placing/sticking the malicious one over the original benign QR code. 2) The attacker manipulates the QR code by changing the color of specific individual modules.

QRishing is a very dangerous and potentially devastating attack that easily be combined with other techniques **[3]**. For example: Selling counterfeited goods, Credential theft, Malicious QR Code that can cause many unimagined damages to the normal common users, for example as in **[5]**: Add a contact listing, Initiate a call, Text someone, Write an email, Make a payment, Reveal user's location, Create a calendar event, Follow Social media account and add a preferred WIFI network. Furthermore, wipe the data on some phones using the Unstructured Supplementary Service Data **(USSD)** codes **[6]** and fool a user to make a payment for a fake service.

As such, just scanning a QR code then, click-and-follow a link is very far from a safe practice, and we can argue that there is a high need for a tool that gives as wise as possible decision to the user. Non-technical approaches exist like users' awareness and training that are necessary but not sufficient without reliance on technical solutions. Blacklisting is the most popular and used anti-phishing technique, however, has many shortcomings, suffers from high false positive rates and subject to obfuscation and evasion techniques.

In this paper, we introduce a POC of Consortium Blockchain-based Whitelisting solution in which unlike Blacklisting solutions, the very nature of exact match of a

URL makes it almost impossible to be evaded when check in a whitelist.

Leveraging the advantages of blockchain technology as distributed with no Single Point of Failure **(SPOF)**, temper-proof, tamper-evident and smart contracts are irreversible and traceable. Consortium blockchain model is permissioned where all nodes and users are known and is not subject to forking.

We envision a network of Business Owners of any type (Companies, Organizations, Small business, Startups, etc.), belonging to varied fields of work (Tourism, Malls, Spare Parts vendors and even coffee shops, etc.), registering their own assets of URLs (long, short, static and dynamic) as such, forming a huge Whitelist of genuine URLs formed by their owners, in addition; authorities audit and regulators oversight is highly recommended.

The rest of this paper organized as follows: section 2) describes what is anti-phishing and what are the current researches, challenges and trends found in the literature, section 3) overall system architecture 4) the proposed solution comprehensive discussion 6) the most relevant related works found in the literature, and finally 7) the conclusion section.

2. Anti-Phishing Current Researches, Challenges and Trends

Although, many anti-phishing techniques are available, with more being developed, none of these are 100% effective **[3]**. Non-technical approaches exist are necessary but not sufficient without reliance on technical solutions. For example, Education and awareness materials targeting users through all types of media and Training programs organizations held for their employees. In addition to, National and International Laws that can play a deterrent role for more casual phishers, but these laws will not deter Advanced Persistent Threats **(APT) [3]**. Following are some major technical trends found in the literature that we classify into two categories: QR Code Relative Solution, and Malicious URL Detection Methods.

2.1 QR Code Relative Solution

- **Visual effects and Masking -** increasing the QR code theme complexity to become harder for an attacker to modify without users unobtrusively notice, and consequently require QR code generators and readers modification/enhancement **[4]**.
- **Embedded Digital Signature** - for example, Quick Response Code Secure **(QRCS)** proposed in **[6]**, is a client-server based cryptographic solution that assures the originator is authentic and the integrity of QR code, to prevent redirecting the users to malicious websites at scanning phase. However, it reduces the area for the actual data to be encoded and QR code readers and generator need to adapt the solution **[4]**.
- **Content Preprocessing -** for the user to preview the contents before connecting, however, it requires some wise user's judgment **[4]**.

2.2 Malicious URL Detection Methods

- **Visual Similarity Detection - Metrics**

To determine the trustworthiness of a URL **[4]**, by computing the visual similarity between features of a suspicious site and a database containing legitimate website features in order to reach metrics, which classify malicious webpages based on exceeding predefined visual similarity threshold. Features include logos, icons, screenshots, and document-oriented models **[3]**, font size, font type, text direction, images and whitelist of Cascade Style Sheet **(CSS)** to check the visited webpage **[7]**. However, this method can be easily bypassed by just slight modification of some visual elements while preserving the overall look or content of the cloned page **[3]** and also Default webpages may not be detected **[7].** From **[8]**, two broad strategies for Malicious URL Detection are used, which are Blacklisting & Heuristics and, Machine Learning **(ML)** for extracting features like (lexical, host-based, content, and others like context and popularity features.)

- **Blacklisting**

Blacklisting phishing domains is the most popular and used technique to prevent the browser to visit a website **[9].** Blacklists are databases that contain known/confirmed malicious URLs. These databases maintained through crowd-sourcing or vendor-based solutions. Upon visiting a URL, the database is queried and warning the user if the URL is found, else if the URL is not found it is treated as benign. Examples are: Google Safe Browsing **(GSB)** a browsers built-in blacklist **[10]**, Microsoft SmartScreen and Defender **[11]**, OpenPhish that uses autonomous algorithms to detect zero day phishing websites, and PhishTank that is community-based voting system for URLs reporting and verification **[10, 12]**. Academic browser-integrated solutions also proposed, like SpoofGuard and PwdHash to mitigate phishing attacks. SpoofGuard raises alerts after checking for phishing symptoms like domain, URL, email, password, links, images and others found in target webpage. PwdHash creates domain-specific passwords that cannot be used if submitted to another domain **[9].** Blacklisting technique is extremely fast - just querying the database - and is very easy to implement. However, Blacklisting has many shortcomings for many reasons:

- Blacklists updating process mostly require human intervention and verification, which may introduce human error **[13]**.
- Blacklists suffer delays and gaps in time to be updated, leaving time for attackers to target victims and users are left vulnerable to attacks for considerable amount of time **[10, 11]**.

- Blacklists differ in update speed and coverage percentage, in addition; blacklists are ineffective in protecting users initially - at hour zero **[13]**.
- Blacklists suffer from non-trivial high false positive and high false negative rates. It is almost impossible to maintain a complete up to date URLs blacklist, since new URLs are created daily, especially when attackers generate new URLs algorithmically which produces a never seen before words/features, then bypass blacklists, making them useless prediction tools on new threats **[8]**.
- Phishing URLs are often short-lived, and blacklists should continually remove such URLs when they are considered no more a threat to increase the blacklists' agility and not to warn users off safe-now websites to decrease its false positives. However, this limits the blacklists' effectiveness and leaves users unprotected for some time. Currently, some major blacklists add again theses URLs if they returned to become or reemerge as a threat, to continue protecting users **[12]**.
- Blacklists have a huge amount of shared/overlapped data, which gives more assurance that a domain is malicious when its entry appears in two or more blacklists **[14]**, hence it is much better querying more than one blacklist if possible but it may be impractical.
- Malvertizing **[3]** can evade blacklists, because it is hard to detect and prevent, as by hosting such malware in a legitimate advertisement-hosting service website, it can be seen as legitimate too and the user will likely click a link. Furthermore, it is hard for the Ad-hosting service to check the legitimacy of each ad redirect **[3]**.
- Importantly, many attackers use obfuscation and evasion techniques to escape for Blacklisting detection **[8, 11]**. In this regard, the work in **[15]** focuses on the significant features that distinguish phishing URLs from legitimate ones, the Age of Domain also is researched in **[16]**, in addition many evading techniques are researched and discussed in **[3, 7, 8, 11, 13, 15, 16, 17, 18, 19]**.

Consequently, it is advised to use Blacklisting in conjunction with other tools, especially ML for increasing the overall performance of the prediction model.

- **Heuristics Approach**

Heuristics are a kind of Blacklisting extension focusing mainly on webpage/website contents by using two methods **[8]**:

1- Building a blacklist of signatures of common attack types. This method is capable of detecting threats in new URLs, however, designed only for a limited of common threats, and obfuscation techniques can bypass them as well.
2- Building a blacklist of signature of a webpage malicious activity such as unusual process creation and repeated redirection. However, this requires visiting the webpage and executing any code and thus, is implemented in destructible virtual machine for safety concerns in case if any launched attack(s). Another drawback is that a malicious website when visited may delay a bit its attack so it may go undetected.

Generally as in Blacklisting, Heuristics suffers from the inability to maintain complete up-to-date lists. In addition, the biggest concern for Vendors is the potential legal liability for mislabeling websites **[13]**.

- **Using Machine Learning (ML)**

ML approaches try to analyze the URL's information and their related websites/webpages, by first extract good feature representations of URLs (static and dynamic), and then train a prediction model using training data that contain malicious and benign URLs, to predict new URLs **[8]** and enhance Blacklisting approaches. Varied machine learning techniques have been researched and implemented, to classify phishing emails, messages, and websites from benign ones, including decision trees, neural networks, and Support Vector Machines **(SVM) [3]**. However, some factors greatly affects the success of ML approaches; updatability should be quick enough, regarding the new training data and trained model and/or the applications updates as new attacks and threats arrive, in addition, different methods used in ML have their benefits, shortcomings, different preprocessing challenges and security concerns **[8]**. Notably, feature representation depends on the amount and quality of the training data, which affects both time and cost. As mentioned in **[8]**, although there are remarkable advancement for malicious URL detection using ML, there still some open problems and challenge exist: 1) Data with high volume and high velocity, 2) Difficulty in acquiring labels, 3) Difficulty in collecting many kinds of features, 4) Feature Representation, 5) Concept drifting and emerging challenges, 6) Interpretability of Models, 7) Adversarial Attacks.

- **Whitelisting**

Whitelisting technique is the opposite of Blacklisting, which is also a database of URLs that are trusted i.e. confirmed to be benign, or fed by the user. For checking a URL, the database is queried and if the URL is found, the target page is loaded otherwise the user is warned. However, as in **[3]**, although the high accuracy rates stated in the researches, it still near impossible to predict what sites the user intents to go to, and any new site even if it is legitimate will be classified as suspicious one. In addition, one of the main obstacles is how to keep updating the contents of the whitelist, and for this reason, auto-upgrade techniques were subject of many researches. Examples of researches found in the literature are discussed in the related work section.

3. Overall System Architecture

We selected IBM Hyperledger Fabric for demonstrating a real-world consortium (permissioned) blockchain network. Hyperledger Fabric is an open source enterprise-grade permissioned blockchain platform established under Linux Foundation. It has a modular architecture with pluggable components and high privacy and security features, so it can be configured and optimized to meet different solution requirements for many use cases in various industries **[20]**.

International Journal of Academic Information Systems Research (IJAISR)
ISSN: 2643-9026
Vol. 6 Issue 11, November - 2022, Pages: 11-18

Our POC consists of three components as in Fig. 1: a) at the left; a webpage for normal users to query the system to check the decoded URL and it interacts with the system through API Gateway. b) at the center; the Hyperledeger Fabric network. c) at the right; a client-side application for authorized users (members, regulators, etc.) to call the smart contract to interact externally with the network and it has the same functions the smart contract provides. Hyperledger Fabric offers a number Application Programming Interfaces **(APIs)** to support developing smart contracts also called (chaincode) and Software Development Kits **(SDKs)** to support developing applications in various programming languages. APIs are available for Go, Node.js, and Java. SDKs are available for Node.js and Java and futuristically in Python and Go **[20]**. Notably; existing systems need not to be rebuilt. Here our focus is on the primary components facility to prove our POC.

In this scene; a URL's owner as a member of the blockchain network using the smart contract, adds its URL asset that intends to embed in a QR code before distribution. A user sees the QR code and if interested scans it then, visit the network's website, copy the encoded URL to check it. In case of the URL exists and benign, the user can go directly to the URL upon desire.

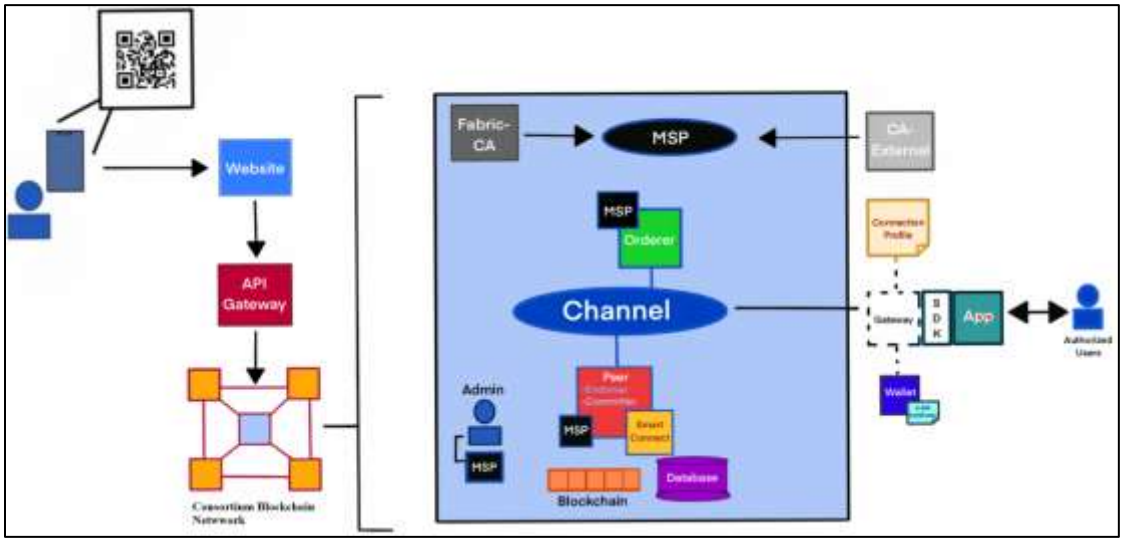

Fig. 1. High Level System Design

4. The Proposed Solution Discussion

We argue in this paper that the prosed solution brings huge value to Anti-QRishing efforts, however, as any information technology field it comes with its own limitations and challenges, as discussed next.

Benefits of the Proposed Solution

1- It is a platform that not manipulated by single entity; but rather, all participants cooperate and collaborate to defend their URLs 'authenticity and legitimacy' and decisions are made through consensus among all of them. In addition, government oversight and intervention where appropriate is highly recommended.
2- Building a Whitelisting overcomes the shortages of using Blacklisting solutions.
3- In Whitelisting approach, the very nature of exact match in URL makes it almost impossible to be evaded that is unlike Blacklisting.
4- Whitelists are by nature proactive and ahead of attackers, unlike blacklists that are by nature reactive and behind attackers.
5- The solution can reach an almost zero detection rates of false positives i.e. wrongly classifying benign URLs into malicious, and false negative i.e. wrongly classifying malicious URLs into benign.
6- Simple to implement, and fast with no scalability issues due to "only query overhead."
7- Periodically can be scanned and revisited by their providers, to make sure that the URLs are live and not stopped or brought down so then can be replaced by malicious URLs.
8- Some blacklists preserve their agility by constantly delisting outdated entries to keep these blacklists current **[19]**. In our proposed solution, the entries are never delisted, only their statuses in case of compromised can be updated as needed, with full history transparency kept. In addition, any future needed fields can be added.
9- Blacklist Vendors can greatly benefit from the solution as it eliminates their biggest concern, which is the potential legal liability for mislabeling websites **[13]**.
10- Support ML solutions and to overcome some of the open challenges via the following:
    - Providing a huge list (could be near complete) of valid URLs including shortened ones, with very

good feature representation and labeling required for models training and fine-tuning, so reducing training efforts in time and cost spent in analyzing billions of data points.
- Can alarm the anti-phishing solution providers with every URL once added, or changed to compromised.
- It can fill the gaps-in-time in case the trained model and/or the applications updates are not soon enough.

11- Permissioned blockchain models have many advantages over permission-less:
- They are not subject to forking (a split or a change to blockchain network's protocol and data structure, leading to have multiple different versions of it to exist at the same time) as nodes and users are all known, all nodes confirm-back ledger updates, and can request software updates thus avoid forking **[23]**. In Hyperledger Fabric it is called "Finality" which means that validated transactions will never be reverted or dropped **[20]**.
- They have no dependency on cryptocurrency and its fluctuating prices, making the majority of costs allocated to infrastructure operating costs **[24]**.

12- Advantage of blockchain technology with its redundant copies in multiple distributed computers, central database that could be SPOF as it can be attacked or compromised and trust in its administrators is a must **[23]**.

13- Blockchain-based systems can prove the existence and hence the ownership of any digital asset at any time. Treating a URL as an asset, increases similarity detection through the execution of a smart contract **[25]**, which determines whether a similar URL exists on the network. In addition, the digital signature in signed transactions further proofs the ownership.

Limitation of the Proposed Solution

1- As in each blockchain use case, the "Network Effect" is the crucial success factor ever, wherein, participants' enthusiasm, corroboration, collaboration and regulators assistance will give great support for the solution deployment, forming a private-public sectors partnership.

2- Some QR code readers perform the necessary action without first getting users' approval **[3]**, and some others still do not support copy and paste operation.

3- In case of compromised website, its status must be urgently changed from benign to suspected, then to malicious or back to benign again, via smart contracts of course.

4- The solution ignores the function of URL ownership transfer cases.

5- It is not claimed to be the bullet proof solution because; attackers, hackers, scammers and phishers are keep innovating to find new ways to overcome existing anti-phishing methods, so it is not the end of the game but a further step to make it far more complicated for them.

6- The solution does not address threats from malware that already infected the user's smart phone.

7- The merit of permissioned blockchain network is that members are trusted and legal agreements to join the network along with its obligations and fines should signed before joining, however it is out-scope of the system.

Suggestions for Future Works and Researches

1- This POC is potentially able to serve other anti-phishing areas: email clients, social media like twitter, browsers, etc.

2- Also, it can include other forms for URLs like digital object identifier **(DOI)**, for example: https://doi.org/10.6028/NIST.IR.8202 used to point to our reference number (23).

3- Researches can help to extend this concept to include other devices for Internet of Things (**IOT)** benefits as well.

4- Enhancing the QR code readers' capability by enabling the users to define the whitelist they wish to go for checking.

5- Practically, not a single blockchain to manage the records of the global population of URLs released in QR code posts is expected. However, having a cross-platform solution and federation of different blockchains implemented on different levels e.g. national, regional and international, working in an interoperable manner without the burden of data replication between one another, eventually making genuine URLs detection globally possible for safe worldwide Anti-QRishing a reality.

6- A number of legal issues may give rise if not used correctly that have to be handled. For instance, although not unique to the proposed system, monitoring the customers' habits like what they prefer, when and where by analyzing what they scan and their location details, etc., can generate revenue by selling such valuable data to third parties without users' consent **[25]** but may violates users' privacy and be subjects to many laws.

7- With the strong security features that blockchain provides e.g. encryption and authentication, any wrong information registered most probably would not be related to hacking the network, but rather mainly due to human errors and/or processes, procedures and working instructions errors, which would require for restrictive governance.

8- In case of unfound-URL, it can be automatically inserted into a suspected-list for investigation, as it may be valid but unregistered URL. Hence, helping in building and updating a blacklist of a "can-be" malicious URLs too.

5. Related Works

From multi perspectives, Whitelisting approach has been subject to many researches in one hand, whether blockchain-based or not and in the other hand whether for anti-phishing or just a pass list or access control.

Examples of Blockchain-based Whitelisting not for anti-phishing:

1. Securing consumer/home-based IOT devices and the networks around them using blockchain technology in **[26]**
2. Using a purpose-based access control scheme implemented by a blockchain system and chaincode to validating doctors' data access with purpose-based consent of patients stored in the blockchain **[27]**.

In addition, examples of researches utilizing whitelist methods for anti-phishing but not blockchain-based:

1- Phishing Detection using Multi-filter Approach **(PhiDMA)**. It is a five layers model: Auto upgrade whitelist layer, URL features layer, Lexical signature layer, String matching layer and Accessibility score comparison layer **[16]**.

2- An Automated Whitelist Approach for detecting phishing attacks in which, the whitelist is determined by carrying out a detailed analysis between the visual link and the actual link **[28]**.

3- Anti-phishing on Automated Individual White-List **(AIWL)** presented in **[29]** to detect phishing and pharming attacks. AIWL automatically tries to maintain a whitelist of all user's familiar Login User Interfaces **(LUIs)** of websites along with their legitimate IP addresses.

4- Using automated individual whitelist to protect web digital identities is presented in **[30]** leverages a Naïve Bayesian classifier to automatically maintain an individual whitelist of a user. Furthermore, it keeps track of the login pages features like IP addresses, Document Object Model **(DOM)** paths of input widgets.

5- PhishBlock A hybrid anti-phishing tool, presented in **[31]**, which is based on both lookup and a SVM classifier that checks features derived from websites URL, text and linkage. The system has three components: Lookup System, Classifier System and Fishblock Checks.

6- An approach using auto-update whitelist of legitimate websites that warn the users is proposed in **[32]**, it employs two components to verify the legitimacy of a webpage: 1) Domain and IP address matching module, 2) Examine the features of the hyperlinks from source code.

7- Model for Assisting Screen-reader users to Phishing Detection **(MASPHID)** is proposed in in **[33],** aiming to help only persons with visual impairments to detect phishing sites, which are aurally similar but visually dissimilar, by assisting persons' screen reader software. If the model did not find a URL in the whitelist, it starts the image based approach.

8- A whitelist based approach for preventing access to phishing sites is presented in **[34]**, that uses URL similarity check to prevent accesses to explicit phishing sites and warns for phishing-suspicious accesses.

9- The work titled "Light weight anti-phishing with user whitelisting in a web browser" is presented in **[35]**, to provide protection for home users, which works on pattern matching method for effective protection and imposing little burden on users.

10- A phishing detection approach called PhishZoo proposed in **[36]** that uses a whitelist containing profiles of trusted websites' appearances to detect phishing and providing a framework for making use of computer vision techniques. It is based on fuzzy hash technique to distinguish content element like HTML code, scripts and images, etc.

Furthermore, presented in **[37],** "PhishChain" a public blockchain-based system to blacklist phishing URLs in a crowd-sourced manner, implemented and managed by a consortium. The goal of PhishChain to assess suspicious URLs found in likely phishing emails. The solution aims to ally the mostly targeted organizations by phishers such as Paypal, Apple, Microsoft and Facebook to form a consortium to put the proposal to use. Any real-world user can join either to submit URLs or verify whether the URL is phishing or not. A page rank-based truth discovery algorithm is proposed to compute URL's phish score and verifier skill points as incentives for participation instead of a cryptocurrency. However, additional mechanisms need to be provided to defend against users maliciously try to manipulate the truth discovery based system.

In this paper, a Permissioned Blockchain-based URL Whitelisting system implemented over Hyperledger Fabric blockchain and owned by a consortium with no crowed-sourcing is proposed. The goal is Anti-QRishing i.e. to check the legitimacy of a decoded scanned QR-code Ad (long, short, static and dynamic.) The consortium members are the URLs' owners, to serve communities and businesses in varied fields such as Banks, Tourism, Malls, Insurance, Small businesses like coffee shops, etc., who make QR-code Ads and want to defend their URLs assets and enable any real-world user to check the legitimacy of their URLs. The incentive is that all members are working for the wellbeing and trustworthiness of the system.

6. Conclusion

In this paper, we introduced a POC of a consortium blockchain-based whitelisting for Anti-QRishing. In Whitelisting solution, the very nature of exact match of a URL makes it almost impossible to be evaded, which is unlike Blacklisting, and almost zero false positives and false negative detection rates can be reached.

Blockchain technology has many advantages as distributed so no SPOF, in addition is temper-proof, tamper-evident and smart contracts are irreversible and traceable. Consortium blockchain model is permissioned so all nodes and users are known, it is not subject to forking, does not depend on a cryptocurrency and not subject for its fluctuation.

In this POC, every URL (long/short, static/ dynamic) is an asset recorded by its member owner for building this whitelist. In this scene; the burden of building a blacklist(s) of invalid URLs or links and keep updating them by security solutions' vendors and non-profit organizations, is replaced by building a whitelist of URLs by their Owners themselves.

Varied URLs owners will benefit to defend their assets of URLs such as Companies, Organizations, Small business, Startups, Doctors, etc., belonging to varied fields of work like: Banks, Tourism, Malls, Insurance, Hospitals, Small businesses and even Coffee shops, who make QR-code Ads for any real-world user to check URLs' legitimacy.

We discussed that non-technical approaches exist that are necessary but not sufficient without reliance on technical solutions. Technical approaches also discussed and focused on Blacklisting that although is the most popular and used anti-phishing technique however, has many shortcomings, suffers from high false positive rates and importantly, are subject to obfuscation and evasion techniques. Benefits, limitations and suggestions for future works and researches also discussed.

Eventually, we argue that the solution is achievable and worth making, but we consider it a complementary rather than substitutional tool of the grate efforts found in the literature.

ACKNOWLEDGMENT

I would like to express my sincere gratitude to both Professor Shawkat K. Guirguis Professor of Computer Science & Informatics, Information Technology Department, Institute of Graduate Studies & Research, Alexandria University and DR. Tamer F. Mabrouk Assistant Professor of Management Information Systems, Egyptian Institute of Alexandria Academy for Management and Accounting, for their great support, guidance and constructive suggestions during the development of this work.

REFERENCES

[1] Computer Security Resource Center (CSRC), glossary, phishing https://csrc.nist.gov/glossary/term/phishing

[2] Vidas, T., Owusu, E., Wang, S., Zeng, C., Cranor, L.F. and Christin, N., 2013, April. QRishing: The susceptibility of smartphone users to QR code phishing attacks. In International Conference on Financial Cryptography and Data Security (pp. 52-69). Springer, Berlin, Heidelberg.

[3] Alabdan, R., 2020. Phishing attacks survey: types, vectors, and technical approaches. *Future Internet*, *12*(10), p.168.

[4] Krombholz, K., Frühwirt, P., Kieseberg, P., Kapsalis, I., Huber, M. and Weippl, E., 2014, June. QR code security: A survey of attacks and challenges for usable security. In International Conference on Human Aspects of Information Security, Privacy, and Trust (pp. 79-90). Springer, Cham.

[5] What You Didn't Know QR Codes Can Do https://www.mobileiron.com/en/qriosity [last visited at 2021/06/29]

[6] Mavroeidis, V. and Nicho, M., 2017, August. Quick response code secure: a cryptographically secure anti-phishing tool for QR code attacks. In International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security (pp. 313-324). Springer, Cham.

[7] Sadiq, A., Anwar, M., Butt, R.A., Masud, F., Shahzad, M.K., Naseem, S. and Younas, M., 2021. A review of phishing attacks and countermeasures for internet of things-based smart business applications in industry 4.0. Human behavior and emerging technologies, 3(5), pp.854-864.

[8] Sahoo, D., Liu, C. and Hoi, S.C., 2017. Malicious URL detection using machine learning: A survey. arXiv preprint arXiv:1701.07179.

[9] Ludl, C., McAllister, S., Kirda, E. and Kruegel, C., 2007, July. On the effectiveness of techniques to detect phishing sites. In International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (pp. 20-39). Springer, Berlin, Heidelberg.

[10] Bell, S., Paterson, K. and Cavallaro, L., 2019. Catch me (on time) if you can: Understanding the effectiveness of twitter url blacklists. arXiv preprint arXiv:1912.02520.

[11] Oest, A., Safaei, Y., Zhang, P., Wardman, B., Tyers, K., Shoshitaishvili, Y. and Doupé, A., 2020. PhishTime: Continuous longitudinal measurement of the effectiveness of anti-phishing blacklists. In 29th {USENIX} Security Symposium ({USENIX} Security 20) (pp. 379-396).

[12] Bell, S. and Komisarczuk, P., 2020, February. An analysis of phishing blacklists: Google safe browsing, openphish, and phishtank. In Proceedings of the Australasian Computer Science Week Multiconference (pp. 1-11).

[13] Steve Sheng, BradWardman, GaryWarner, Lorrie Faith Cranor, Jason Hong, and Chengshan Zhang. 2009. An empirical analysis of phishing blacklists. Proceedings of Sixth Conference on Email and Anti-Spam (CEAS) (2009).

[14] Marc K¨uhrer and Thorsten Holz. 2012. An empirical analysis of malware blacklists. PIK-Praxis der Informationsverarbeitung und Kommunikation 35, 1 (2012), 11–16.

[15] Jeeva, S.C. and Rajsingh, E.B., 2016. Intelligent phishing url detection using association rule mining. Human-centric Computing and Information Sciences, 6(1), pp.1-19.

[16] Sonowal, G. and Kuppusamy, K.S., 2020. PhiDMA–A phishing detection model with multi-filter approach. Journal of King Saud University-Computer and Information Sciences, 32(1), pp.99-112.

[17] Jones, R., 2005. Internet Forensics. [online] O'Reilly Online Learning. https://www.oreilly.com/library/view/internet-forensics/059610006X/ch04.html

[18] Rathod, J. and Nandy, D., 2014. Anti-phishing technique to detect URL obfuscation. Int. J. Eng. Res. Appl., 4(5), pp.172-179.

[19] Kührer, M., Rossow, C. and Holz, T., 2014, September. Paint it black: Evaluating the effectiveness of malware blacklists. In International Workshop on Recent Advances in Intrusion Detection (pp. 1-21). Springer, Cham

[20] hyperledger-fabricdocs Documentation - Release master v2.x, Sep 30, 2020 https://hyperledger-fabric.readthedocs.io/_/downloads/en/v2.2.1/pdf/

[21] Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y. and Muralidharan, S., 2018, April. Hyperledger fabric: a distributed operating system for permissioned blockchains. In Proceedings of the thirteenth EuroSys conference (pp. 1-15).

[22] Iftekhar, A., Cui, X., Tao, Q. and Zheng, C., 2021. Hyperledger fabric access control system for internet of things layer in blockchain-based applications. Entropy, 23(8), p.1054. https://mdpi-res.com/d_attachment/entropy/entropy-23-01054/article_deploy/entropy-23-01054-v2.pdf

[23] Yaga, D., Mell, P., Roby, N. and Scarfone, K., 2018. Blockchain Technology Overview (NISTIR-8202). NIST: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8202

[24] Jesus Ruiz. Public-Permissioned blockchains as Common-Pool Resources. [Technical Report] Alastria Blockchain Ecosystem. 2020. ⟨hal-02477405⟩ https://hal.archives-ouvertes.fr/hal-02477405/document

[25] Qureshi, A.; Megías, D. Blockchain-Based Multimedia Content Protection: Review and Open Challenges. Appl. Sci. 2021, 11, 1. https://dx.doi.org/10.3390/app11010001

[26] Mendez Mena, D.M. and Yang, B., 2018, September. Blockchain-based whitelisting for consumer IoT devices and home networks. In *Proceedings of the 19th Annual SIG Conference on Information Technology Education* (pp. 7-12).

[27] Tith, D., Lee, J.S., Suzuki, H., Wijesundara, W.M.A.B., Taira, N., Obi, T. and Ohyama, N., 2020. Patient consent management by a purpose-based consent model for electronic health record based on blockchain technology. *Healthcare Informatics Research*, *26*(4), pp.265-273.

[28] Azeez, N., Misra, S., Margaret, I.A. and Fernandez-Sanz, L., 2021. Adopting Automated Whitelist Approach for Detecting Phishing Attacks. Computers & Security, p.102328.

[29] Cao, Y., Han, W. and Le, Y., 2008, October. Anti-phishing based on automated individual white-list. In Proceedings of the 4th ACM workshop on Digital identity management (pp. 51-60).

[30] Han, W., Cao, Y., Bertino, E. and Yong, J., 2012. Using automated individual white-list to protect web digital identities. Expert Systems with Applications, 39(15), pp.11861-11869.

[31] Fahmy, H.M. and Ghoneim, S.A., 2011, March. PhishBlock: A hybrid anti-phishing tool. In 2011 International Conference on Communications, Computing and Control Applications (CCCA) (pp. 1-5). IEEE.

[32] Jain, A.K. and Gupta, B.B., 2016. A novel approach to protect against phishing attacks at client side using auto-updated white-list. EURASIP Journal on Information Security, 2016(1), pp.1-11.

[33] Sonowal, G. and Kuppusamy, K.S., 2016, August. Masphid: a model to assist screen reader users for detecting phishing sites using aural and visual similarity measures. In Proceedings of the International Conference on Informatics and Analytics (pp. 1-6).

[34] Kang, J. and Lee, D., 2007, November. Advanced white list approach for preventing access to phishing sites. In 2007 International Conference on Convergence Information Technology (ICCIT 2007) (pp. 491-496). IEEE.

[35] Wang, Y., Agrawal, R. and Choi, B.Y., 2008, April. Light weight anti-phishing with user whitelisting in a web browser. In 2008 IEEE region 5 conference (pp. 1-4). IEEE.

[36] Afroz, S. and Greenstadt, R., 2011, September. Phishzoo: Detecting phishing websites by looking at them. In 2011 IEEE fifth international conference on semantic computing (pp. 368-375). IEEE.

[37] Edirimannage, S., Nabeel, M., Elvitigala, C. and Keppitiyagama, C., 2022. PhishChain: A Decentralized and Transparent System to Blacklist Phishing URLs. arXiv preprint arXiv:2202.07882.