HIGH SCHOOL EDITION
Journal of Student Research
Volume 14 Issue 1 (2025)

Phishing Attacks and Defense Strategies in Bitcoin and Ethereum: A Comparative Review

Neil Soman

Hamilton High School, USA

ABSTRACT

Phishing is a serious threat to cryptocurrency networks; Bitcoin and Ethereum are prime targets for these attacks. This paper discusses some aspects of phishing attacks on these platforms. While the simpler architecture of Bitcoin leads to more direct phishing attempts, the more complex ecosystem in Ethereum introduces a wide range of attack vectors through dApps and smart contracts. A comparative analysis of phishing attacks in both blockchains shows that while both have their fair share of attacks, Bitcoin seems to bear the brunt of phishing attacks. Current defense strategies, like 2FA and anti-phishing tools, as well as recommendations for increasing network security against phishing are discussed in this paper. Understanding these phishing mechanisms is crucial in strengthening the security of blockchain platforms and mitigating future attacks.

Introduction

Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords, and financial details by disguising it as a trustworthy entity in electronic communications. It can be carried out through methods such as fake emails, deceptive websites, and malicious attachments. Victims often fall for these scams by clicking on links or providing personal information without verifying the source, which allows malicious entities to gain access to their data. These attacks can result in severe consequences, including financial losses, identity theft, and unauthorized access to personal or corporate accounts. The danger of phishing lies in not just the presence of vulnerabilities in the system, but also in human inattention. Usually, phishing utilizes social engineering tactics, relying on human gullibility rather than hardware or software flaws to succeed.

With the increasing popularity of blockchain networks like Bitcoin and Ethereum for transferring money and other digital assets, these platforms have become prime targets for phishing attacks. Unlike traditional financial systems, blockchain networks operate on a decentralized framework, eliminating control by a single entity. This decentralization reduces the risk of fraud, and increases transparency, as all transactions are carefully recorded on a publicly accessible ledger. One caveat to this approach, however, is that these networks lack a central authority capable of taking preventive and corrective actions against such attacks, making it challenging to defend against phishing and leaving users more vulnerable.

This paper focuses on educating individuals about the different types of phishing attacks and how to defend against them effectively. The structure of the paper is as follows: first, an in-depth analysis of various phishing attack techniques, detailing their mechanisms. Next, the architectures of the Bitcoin and Ethereum will be explored, emphasizing their distinctive features. Following this, the paper will analyze the differences in phishing attacks targeting Bitcoin and Ethereum. Finally, recommendations for enhancing defenses against phishing attacks on these blockchain platforms will be proposed.

Through this comprehensive examination, the paper aims to equip readers with the knowledge needed to recognize and mitigate phishing threats in blockchains, thus leading to a more secure digital environment

What is Phishing

Definition

The issue of phishing lacks a precise definition because it encompasses a wide range of scenarios and tactics. For example, Colin Whittaker et al. [1] define phishing as:
"We define a phishing page as any web page that, without permission, alleges to act on behalf of a third party with the intention of confusing viewers into performing an action with which the viewer would only trust a true agent of the third party."

This definition does indeed capture the deceptive nature of phishing attacks, emphasizing the role of impersonation in misleading victims. However, it still has limitations, as it only defines phishing as scenarios involving third-party impersonation, which does not account for all types of phishing attacks.

PhishTank, an anti-phishing platform that offers a community-driven system for verifying phishing attempts, on the other hand, offers a more focused definition, describing phishing as a fraudulent attempt, usually made through email, to steal personal information. This definition is rather narrow and points out one of the common methods: attacks on personal data. It does explain a lot of phishing attacks, but it does not cover all phishing activity. For instance, phishing can also be used to lure victims into downloading malware that conducts some action, without necessarily stealing any personal information.

Both these definitions have some truths but also major limitations. Whittaker's definition broadens the concept of phishing from mere stealing of personal information to include the actionable elements of deception that mislead victims, however it does not capture scenarios when the attackers do not impersonate third parties. On the other hand, PhishTank's definition, that captures the essence of email-based phishing that is aimed the theft of personal data, relates to other sophisticated methods where using malware makes it possible to achieve the attacker's goals.

To better address the complexities of phishing, a more comprehensive definition is needed.
According to Mahmoud Khonji et. al. [2]:

"Phishing is a type of computer attack that communicates socially engineered messages to humans via electronic communication channels in order to persuade them to perform certain actions for the attacker's benefit."

These messages fool victims into performing actions that benefit the attacker but do not show the benefit to the attacker. For example, a phishing attack could trick an employee into downloading a malware-infected attachment by convincing them that they are to download an important document, which in turn initiates a ransomware infection. This more general definition includes the many different tactics and goals of phishing.

Background

History of Phishing

According to Koceilah Rekouche [3], the history of phishing traces back in important ways to the mid-1990s when hacking software facilitated the mass targeting of people in password stealing scams on America Online (AOL), an Internet service provider and web portal that was popular in the late 1990s and early 2000s due its delivery of dial-up Internet access, web services, and digital content. At its emergence, phishing, usually against America Online accounts, would involve users being tricked into giving personal information through misleading messages. This method is thus appropriately named, comparing attackers to fishers who bait hook their prey. The essence of phishing, though, is deceit, which leads to the disclosure of a user's sensitive data.

By 1997, phishing had evolved and turned into a resourceful activity where huge amounts of stolen accounts became valuable assets for hacker communities. In other words, it meant a very distinct shift in the attack focus—the cybercriminals no longer threatened only single accounts but also much more profitable sources of financial gain, such as online banking and e-commerce services. The fact that phishing's scope of application started to grow showed an increasingly sophisticated threat with growing relevance for these new, high-value targets.

As these tactics kept getting mature, the focus of the attacks widened from users to the employees of organizations. This surely means that it had been a strategic shift when it was desired to compromise the whole system and not just the account of a person. Modern phishing mechanisms represent this maturity, such as Man-in-the-Browser, which uses much more sophisticated methods to bypass safety measures and protect sensitive information.

Motivations Behind Phishing

Phishing attacks could be driven by several objectives, all reflecting the different goals of cybercriminals.

Yu et al. outlined eight motives from an attacker's perspective behind phishing [4]:

1. Financial gain
2. Exploiting security vulnerabilities
3. Trafficking of identities
4. Seeking fame and recognition
5. Conducting industrial espionage
6. Collecting passwords
7. Distributing malware
8. Committing identity theft

According to Vega et. al. [5], the most common motive for an attacker is financial gain. Attackers often make a website and disguise themselves as legitimate financial institutions to acquire victims' banking credentials, which they use to siphon funds or conduct unauthorized transactions. Identity theft, closely associated with financial gain, involves stealing personal information to impersonate the owner and commit fraud. This stolen information can be resold in underground markets or used in further criminal activities.

Beyond direct financial incentives, identity trafficking is another motive where phishers sell stolen identities to criminals who seek to pose as others to hide their real identities and activities. This enables illegal actions, such as purchasing goods anonymously. A more sophisticated motive involves industrial espionage, where attackers target key individuals or groups within an organization to obtain sensitive information. Such typical industrial espionage attacks using phishing include spear-phishing and whaling. In these methods, the attackers would very specifically go after high-value targets - or even mid-level corporate employees - in order to infiltrate corporate networks.

Some phishers are motivated by the desire for fame or reputation within their peer communities. Successfully launching an attack can enhance an individual's stature within a group of hackers. Additionally, some phishers aim to distribute malware through phishing emails. This malware infects victims' systems and can later be used to harvest passwords, monitor user activities, or gain unauthorized access to further resources.

Another motive is exploiting security holes. Phishers search for and exploit vulnerabilities in systems or networks to maximize the success rate of their attacks. Understanding these different motives enables cybersecurity professionals to develop more targeted and effective prevention and mitigation strategies against this multifaceted threat.

Attackers are driven by a range of motives, from financial gain and identity theft to more sophisticated goals like industrial espionage and exploiting security vulnerabilities. Each motive underscores the diverse and complex nature of phishing attacks and provides an innuendo into the tactics used by attackers. Understanding these motives is crucial for identifying phishing attempts and developing effective strategies to combat them.

Types of Phishing

There are two main types of phishing attacks, social engineering-based attacks and technical-based attacks. According to Jagatic et. al. [6], social engineering schemes are based on deception and subsequent independent wrong actions of the victim. On the other hand, technical schemes use vulnerabilities and imperfections of software and infrastructure [7].

Social Engineering-Based Attacks

Social engineering-based attacks rely solely on the user of a network. For instance, an attacker could act as a high-ranking executive, say the CEO, sending an urgent, spoofed email to a targeted employee for help in opening an unmarked file (this could lead to the opening of the file and an injection of a piece of malware or virus into the employee's system).

Table 1. Examples of Social-Engineering Phishing Attacks

Type of Social Engineering-Based Attack	**Famous example**	**Description of the attack**
Email Phishing	Target Corporation (2013)	Scammers created a replica of the Target login page using a phishing attack that convinced people into submitting their credit card information. The fraudulent website took personal data and card details, from which millions of dollars were later stolen.
Spear Phishing	John Podesta (2016)	Attackers sent a speared email pretending to be from Google to John Podesta (the senior advisor to the democratic president), tricking him into revealing his email password. This credential theft compromised sensitive information and contributed to a larger cyber attack on the 2016 Clinton campaign.
Whaling	Jeff Bezos Phone Hacking Incident (2018) [8]	In 2018, Jeff Bezos, the CEO of Amazon, was targeted in a phishing attack when he received a malicious video file via WhatsApp, supposedly from Saudi Crown Prince Mohammed bin Salman. The file contained spyware that exploited a vulnerability in the app, allowing attackers to access and extract private data from Bezos's phone
Fake ICO	Centra Tech (2018)	Fraudsters launched a fake ICO for a cryptocurrency startup, promising high returns to investors. The professional-looking website and whitepaper convinced investors to transfer cryptocurrency to a scam wallet, resulting in millions of dollars lost to the scheme.
Smishing	HMRC UK (2016)	Attackers sent smishing texts posing as Her Majesty's Revenue and Customs (HMRC), claiming a tax refund was due. The messages included a link to a fake HMRC site that collected personal and financial details, leading to significant identity theft and financial fraud.

Clone Phishing	Epsilon Data Breach (2011) [9]	Following a major data breach at Epsilon, attackers cloned legitimate emails from the various clients of Epsilon, and embedded malicious links. These clone phishing emails tricked recipients into giving up personal and financial information on fake websites.
Pharming	MyEtherWallet (2018)	Hackers tampered with DNS settings to redirect users from the legitimate MyEtherWallet website to a fraudulent clone. Victims entered their wallet credentials on the fake site, allowing attackers to steal private keys and drain cryptocurrency funds totaling hundreds of thousands of dollars.
Angler Phishing (Social Networking)	British Airways (2018)	Attackers set up fake customer-support accounts on Twitter, copying British Airways' support profile, and tricking the target users into revealing sensitive information or clicking links to malicious sites under the guise of resolving service issues. This led to the exposing of user's personal information.

This chart is inspired by the work done by Andryukhin [7]

Phishing Emails: This widely used phishing technique involves sending deceptive emails that appear to originate from trusted organizations like banks or popular websites. Attackers craft e-mails, making it look like it is from an authentic source, and they usually use language that will trigger the recipient into taking action. These emails might have malignant links or attachments that are supposed to capture personal information or download malware. By leveraging the familiarity and trust associated with known brands, phishers exploit recipients' confidence to gain unauthorized access to sensitive data.

Spear Phishing: This type of email phishing involves an attack on a particular individual or organization. Attackers gather specific details about their target in a campaign from social media, other public sources, or anywhere else; all this is to present a convincing and personalized attack. These messages are highly personalized and attempt to come across as being sent from something to which the user would feel an inherent sense of responsibility in answering; these emails often request confidential information or ask the target to carry out actions that could compromise their security. The precision and personalization of spear phishing make it particularly effective and challenging to detect.

Whaling: This is another variation of spear phishing that targets high-profile people, mainly executives or senior managers. Attackers customize the phishing attempt with detailed information about the targeted high-profile individual and his or her job role. To do this, the attacker can use the identity of a high-ranking staff member, creating an illusion of importance. An example of a whale attack could involve an attacker impersonating a CEO and requesting a substantial financial transaction from the CFO. This approach leverages high-ranking officials' authority and associated trust to access sensitive corporate data or financial resources.

Vishing: Attackers use phone calls or some form of telecommunication to impersonate banks, customer service, or any other form of organization that is likely to ask for sensitive information from an individual in use of their service. They use phone calls and social engineering to get personal information, such as account numbers or Social Security numbers. By creating a sense of urgency or using emotional manipulation, vishers are able to extract sensitive data from their targets.

Smishing: This form of phishing targets users through SMS (text messages) that are impersonated as coming from official sources. Counterfeit links or requests for personal information often make it to the target's device. Smishing leverages that text messages seem to be more urgent than emails, according to people's perception, and are not looked

at closely. The result, therefore, is that victims are more likely to click unverified links or provide sensitive information without confirming who the sender is.

Clone Phishing: Clone phishing is a technique in which attackers replicate genuine emails that their victim has received earlier. The cloners change the content of the email, such as links or attachments, so that when opened or clicked, it would lead the victim to some malicious resources. By sending this modified email to the victim, attackers exploit users' familiarity with the original message, making it more difficult for them to recognize the fraudulent nature of the email. This tactic takes advantage of the victim's prior trust in the original email.

Pharming: In a pharming attack, users are redirected from a legitimate website to its clone without knowledge of the redirection. For this to happen, attackers either poison DNS servers or infect client computers with malware that changes browser settings. The users that are redirected could then offer their sensitive information on a fraud site, which usually exactly resembles the original website. Pharming attacks, when done right, can be very dangerous as they target multiple victims simultaneously, and in most cases are difficult to detect—the phishing site looks similar to the real site.

Angler Phishing: In this relatively recent type of attack, phishers create fake customer service accounts on social media platforms or hijack existing ones to engage with their users. By posing as customer support representatives, they get users to click on malicious links or give away information. This method can take advantage of the trust you have in the official support channel, with interactions that appear to be normal customer service, either to steal sensitive data or to distribute malware.

Homograph Attacks: Phishers create fraudulent websites or fake pages with URLs that closely resemble those of legitimate sites. These attacks often use Punycode encoding to register domains with characters that appear similar to standard Latin letters but are different. For instance, it is possible to register domain names in Cyrillic characters that are virtually indistinguishable from the standard Latin graphics. This is just an instance of visual similarity that may deceive users to believe they are navigating to a legitimate website; therefore, it is important to pay attention while checking the URLs, in order to make a differentiation of which ones are legitimate or fraudulent.

Fake ICOs: According to Andryukhin [7], "ICOs (Initial Coin Offerings) are the dream of any hacker. Lightning fast, often quite simple attack on cryptocurrency services and block-start-ups brings millions of dollars of profit with minimal risk for criminals [10]". Scam ICO projects that lack any real product or development team entice investors with false promises of high returns. They set up convincing project pages, often including promotional videos and whitepapers, and actively promote their schemes through media coverage and personal meetings. Additionally, scammers may hack databases of genuine ICOs to target early investors, offering them attractive but fraudulent investment opportunities.

Technical-Based Attacks

Table 2. Examples of Technical-Based Phishing Attacks

Type of Technical-Based Attack	Famous example	Description of the attack

DNS Spoofing (DNS Cache Poisoning)	Brazilian Bank Attack (2010)	In 2010, attackers successfully carried out DNS cache spoofings of various Brazilian banks. The attackers poisoned the DNS entries such that any user trying to access the legitimate bank websites was instead sent to malicious sites, which would enable the attackers to steal users' sensitive information and access to bank accounts
Man-in-the-Middle (MitM) Attacks	The Superfish Incident (2015)	Lenovo laptops were found to have pre-installed adware called Superfish, which acted as a man-in-the-middle by intercepting and decrypting HTTPS traffic. This adware inserted its own root certificate into the system, allowing it to decrypt encrypted web sessions. Through this adware, attackers could eavesdrop on users' private communications and potentially steal sensitive information.
Malware-Based Phishing	The Zeus Trojan (2007)	The Zeus Trojan Virus was a malware program that originally emerged in 2007 and infected millions of computers worldwide. This malware captured keystrokes and login details, with particular mention of banking details. By logging keystrokes and screenshots, attackers were able to steal victims' online banking details and transfer funds from their accounts.
Evil Twin Attack	Starbucks Wi-Fi Incident (2017)	Attackers in 2017 deployed a rogue Wi-Fi access point to spoof the legitimate Starbucks network. Once customers were connected to this fake network, their internet traffic was intercepted and monitored by an attacker. This allowed the attackers to sniff login credentials and other private information that passed through the network

This chart is inspired by the work done by Andryukhin [7]

DNS Spoofing (DNS Cache Poisoning): Attackers corrupt the DNS server's cache by inserting false information, causing users to be redirected to fraudulent websites without their knowledge. This technique exploits weaknesses within the DNS protocol, redirecting visitors of legitimate sites to bad actors' sites.

Man-in-the-Middle (MitM) Attacks: In these attacks, the attacker intercepts and alters communication between two parties without their knowledge. This could be done either by exploiting insecure protocols in a network or through malware that can sniff and manipulate data during transmission to acquire sensitive information.

Malware-Based Phishing: Attackers use malware to execute phishing schemes. The malware can be delivered via email attachments, malicious downloads, or infected websites. Once installed, it can capture keystrokes, steal credentials, redirect web traffic, or create backdoors for remote access.

Evil Twin Attack: In this attack, a rogue Wi-Fi access point is set up by the attacker to mimic a legitimate one. When users connect to the fake access point, the attacker can intercept and manipulate the data transmitted over the network, gaining sensitive information such as login credentials or financial data.

Overview of the Structures of the Bitcoin and Ethereum

Introduction to Blockchain Technology

According to Sarmah et al. [11], blockchains are databases of records of transactions that are distributed, and at the same time they are validated and maintained by a network of computers around the world.

Blockchains are based on a decentralized structure, using a peer-to-peer network. This means that rather than relying on a single central authority like a bank or government, blockchain technology operates under the supervision of a vast community, ensuring that no single individual has control over the entire system. In essence, while a typical centralized database is housed on a single server, blockchain spreads its information across all users of the software. This decentralization allows every participant in the network to view everyone else's entries, preventing any one entity from seizing control. When a transaction is initiated, it is broadcasted to the network, where computer algorithms assess its validity. Once verified, this transaction is connected to previous ones, creating a continuous chain of linked transactions, aptly named the blockchain. This makes it almost impossible for anyone to retroactively alter or erase transaction histories. Unlike traditional centralized databases, where information is stored on a singular server, blockchain's distributed nature ensures that data cannot be manipulated. This structure is reinforced by peer verification, providing strong guarantees of accuracy.

The Blockchain Architecture in Short

The architecture of a blockchain network is usually divided into three sections: Applications, Decentralized Ledger, and Peer-to-Peer Network [11]. Each of these layers specifies a different way to interact with and manage the blockchain network.

Applications: The application layer is "the business logic for digital asset transactions and the execution of smart contracts" [12]. This layer represents the various tools, platforms, and software that users interact with, enabling them to utilize the blockchain for specific purposes, such as executing smart contracts or performing transactions.

Decentralized Ledger: A decentralized ledger "is a consensus of replicated, shared, and synchronized digital data that is geographically dispersed (distributed) across many sites, countries, or institutions" [13]. It ensures that every transaction is verifiable and permanently stored across the entire network without relying on a central authority.

Peer-to-Peer Network: This layer specifies how the blockchain operates and communicates across a distributed network of nodes. It allows all participants to share and verify information directly with one another, ensuring the network remains decentralized and resilient against failures or attacks. "Blockchain allows to securely store, using cryptography functions, validated transactions and other data across its peer-to-peer (P2P) network" [14].

Types of Blockchains

Since the release of Satoshi Nakamoto's novel 2008 paper, "Bitcoin: A Peer-to-Peer Electronic Cash System" [15], blockchain technology has evolved into various forms, each with distinct characteristics and specific use cases.

Public Blockchains: These are open and decentralized networks where anyone can participate by validating transactions and accessing the blockchain. Examples include Bitcoin and Ethereum.

Private Blockchains: These blockchains are controlled by a single organization and are usually used internally. Access is restricted, and only specific users are allowed to participate. An example would be Hyperledger.

Consortium Blockchains (Federated Blockchains): These blockchains are semi-decentralized, and controlled by a group of organizations rather than a single entity. They are often used in industries where collaboration between multiple entities is required, like banking.

Hybrid Blockchains: A combination of public and private blockchains, hybrid blockchains allow certain data to be kept private while other data is made public. They offer flexibility in terms of what is shared and who has access.

Sidechains: These are separate blockchains that run parallel to the main blockchain, allowing assets to be transferred between them. Sidechains enable experimentation and the implementation of features not available on the main blockchain.

Advantages of Blockchain Over Fiat Money

Immutable Transaction Records: Blockchain technology irrevocably handles transactions to ensure that whatever happens is not tampered with or deleted. This will provide an immutable, perfect record of all activities, hence enhancing trust and accountability. [11]

Resilient Network Architecture: By design, blockchain does not have single nodes of failure, and it allows the network to handle security attacks and stay on even when some of the nodes are compromised, which in turn gives it very high reliability even under very adverse conditions. [16]

Enhanced User Control and Traceability: With this, users will have more control over their information and transactions, being able to trace the history of any kind of transaction with digital stamps. This allows for maximizing the end user's confidence that it can be proven they did everything accurately.[17]

Fraud Detection and Security: The peer-to-peer nature of blockchain networks not only helps in detecting fraudulent activities but also adds to the security of the system, wherein control over half of the nodes is needed to do anything that will significantly harm or manipulate the network. This distributed consensus mechanism acts as a strong deterrent to possible attackers. [17]

Secure and Redundant Data Storage: The fact that blockchain distributes data across several copies makes it less risky to have sensitive information stored in one location, while its end-to-end encryption would be sure to secure sensitive business data. This model of distributed storage also offers improved data redundancy and accessibility. [16]

Trusted and Reliable System Adoption: The high level of security and trust offered by blockchain systems makes them more reliable for users and customers. As a result, blockchain is increasingly being adopted across various industries where data integrity and security are paramount. [16]

Challenges of Blockchains

Integration Challenges: Blockchain integration with existing systems is not easy. It requires a lot of changes that are costly and time-consuming. At the organizational level, proper planning in terms of resource allocation for maintaining coherence with the present infrastructure is usually bridging the technical and operational gaps.

Environmental Impact: High energy consumption, associated with blockchain, mainly in the proof-of-work(PoW) system underlying Bitcoin, has brought several environmental concerns to the fore. There is a migration underway toward more energy-friendly consensus mechanisms, such as Proof of Stake; however, it is slow and contested by established networks.[18]

Security Vulnerabilities: Especially the smaller blockchain networks are susceptible to the 51% attack, whereby some entity takes control of the majority in a blockchain network. This kind of attack is dangerous to the integrity and security of the blockchain, whose compromise can be quite dangerous to the users.

Low Scalability: Most of the blockchain networks face problems with speed and efficiency when they grow. For example, increasing numbers of transactions in the case of Bitcoin will overload the system, slowing down the times

of processing and increasing fees connected with them. Experimented solutions involve the implementation of sharding and layer 2 technologies; still, they add further complexity to the network. [19]

Technical Complexity: The complexity of blockchain technology itself is a barrier to its mass diffusion because it requires that users have high levels of technical expertise. This complexity is scaring business enterprises and individuals from adopting blockchain, hence affecting its potential impact in various business industries.

High Costs of Implementation: Setting up a blockchain system and its subsequent development requires a substantial upfront investment in technology and qualified personnel. In most cases, these high costs of implementing blockchain solutions are quite prohibitive to many organizations, more so the small ones, thereby limiting the possibility of its wide diffusion. [20]

Regulatory Uncertainty: Evolving and often unclear regulations create an unpredictable environment for blockchain adoption. This becomes challenging to ensure compliance with local and international laws, which sometimes vary too widely and change rapidly to ensure the stability and growth of blockchain projects.

Interoperability Challenges: This has long meant running parallel blockchain networks unable to intercommunicate and share data, which also limits the broader use of the technology. Several efforts are underway to create cross-chain solutions, but it still remains among the major challenges that, once solved, will improve the growth of decentralized ecosystems.

Introduction to Bitcoin

One of the most well-known approaches to the concept of blockchain technology is Bitcoin. First brought into light by Satoshi Nakamoto's 2008 paper, "Bitcoin: A Peer-to-Peer Electronic Cash System" [15], Bitcoin represented the first implementation of blockchain technology.

Bitcoin is a peer-to-peer network of electronic cash, enabling online payments to be transferred directly between parties without the need for a financial institution [21]. To be able to transfer payments without the need for a trusted third party (like a bank or governing body), Bitcoin utilizes a decentralized digital ledger system. As described by Vujičić et al. [22], The Bitcoin digital "ledger is defined as a state transition system, consisting of a state that shows ownership status of all existing bitcoins and a state transition function, in the form of a transaction". In short, Bitcoin's digital ledger is a public, decentralized record of all Bitcoin transactions that have ever occurred.

How Does Bitcoin Work?

In order to transfer bitcoins (BTC), users interact with software known as "wallets." A Bitcoin wallet is a digital tool that allows users to store, send, and receive bitcoins securely. It functions as an interface between users and the Bitcoin network, enabling them to manage their Bitcoin holdings and transactions efficiently. [23]

A Bitcoin wallet does not actually store bitcoins themselves; rather, it stores the cryptographic keys that provide access to the bitcoins recorded on the blockchain. There are two types of keys associated with Bitcoin wallets: public keys and private keys. The public key acts like an address that others can use to send bitcoins to the wallet, while the private key is a secret code that allows the wallet owner to access and control their bitcoins. [24]

Instead of relying on common bank and processor intermediaries, Bitcoin uses cryptographic techniques for one-party-to-another-party transactions directly over the internet. A single digital signature accompanies each transaction completed, created by a sender using his private key and validated using the public key of the receiver. Each transaction bearing ownership of a portion of the cryptocurrency requires the sender to verify his private key corresponding to the input.

When a digital payment is received, the recipient's system verifies the authenticity of the digital signature against the sender's public key. In doing so, it assures the recipient that the transaction was truly authorized by the holder of the corresponding private key.

After it passes the authentication checkpoint, the requested transaction is shown on every part of the Bitcoin network so that nodes, individual computers on a network that all hold identical copies of the blockchain database [25], can verify the transaction.

A verifying node needs to identify two main points of information about a requested transaction [26]:

1. That the spender of an amount of BTC (Bitcoin's currency) has sufficient funds in their account. This is done by checking every appearance of a spender's public key on the Bitcoin digital ledger and tracing exactly how much funds the spender has in their account.
2. That the requested transaction was verified to be accepted by the two parties involved.

How Does Bitcoin Solve the Problem with Achieving Consensus Between the Network of Nodes in A Decentralized System? Because transactions are forwarded from node to node in the Bitcoin network, their order of arrival at any particular node will not necessarily be the order in which they were created. The sequence in which they were created must therefore be determined to provide consensus across the Bitcoin network. In order to solve this issue, Bitcoin uses Blockchain. At its core, Bitcoin structures transactions into lots called blocks. Each transaction is recorded in a "block," and these blocks are linked together in chronological order, forming a "chain" of blocks, hence called Blockchain. This structure treats all transactions within one block as simultaneous events. [27]

To tackle the challenge of multiple blocks being proposed for the same transaction by different nodes simultaneously, Bitcoin employs a mechanism known as "proof of work." [28] This approach requires that a block can only be accepted into the Blockchain if it contains a solution to a complex mathematical puzzle. For example, nodes may need to discover a "nonce" value that, when combined with the transactions and hashes of previous blocks, results in a hash with a predetermined number of leading zeros. This process ensures that high computational effort will be used with each block to make sure that blocks are valid, thus keeping the integrity and consistency of the Blockchain as a whole.

Benefits of Bitcoin

According to Fauzi et al. [29], Bitcoin offers numerous potential benefits and future applications despite its significant price increases and rising value, particularly through its secure technology, cost-effective transactions, and potential for high returns.

Firstly, Bitcoin's secure technology is primarily driven by its blockchain infrastructure. Blockchain's decentralized architecture with the overlay of advanced cryptographic techniques makes any transaction immutable and resistant to tampering or fraud [30]. Bitcoins derive their security from their proof of work (PoW) mechanism. The mechanism involves miners who solve complex mathematical problems in order to validate transactions and add new blocks to the blockchain. It is precisely this tremendous need for computational resources in the puzzles that poses an imposing barrier to malice: any attempt to alter this blockchain would require re-solving the puzzles for all subsequent blocks—computationally infeasible—in order to maintain a valid blockchain copy.

Secondly, compared to legacy financial systems, Bitcoin ensures low-cost transactions. By getting rid of most of the middlemen, Bitcoin not only speeds up the processing of transactions but also drastically reduces transaction fees. Unlike traditional methods of payment, which charge many layers of fees—banks, credit card operators, and settlement processors, for example—Bitcoin transactions usually mean lower costs, mostly for overseas transactions. In this respect, this efficiency benefits individuals and businesses alike through reduced expenses for transactions and eased financial operations.

Finally, there is huge potential in terms of high returns on investment in Bitcoin. Its decentralized nature and capped supply of 21 million bitcoins [15] make it a greater hedge against inflation and a better store of value. Historical price growth was quite considerable for Bitcoin, making it very attractive to investors who want huge returns. Though

the volatility of the currency brings risks, this also provides an opportunity for high gains. Its value may rise further with increasing adoption and institutional interest, establishing its position as a very valuable asset in one's investment portfolio.

Bitcoin, like many other blockchains, was designed to serve a specific niche within the global landscape. Created by Satoshi Nakamoto, Bitcoin was introduced as a way to carry out transactions between individuals and corporations quickly, safely, and anonymously [31]. Bitcoin's features present promising opportunities. Using its unique ledger system, blockchain technology, and verification system, Bitcoin is able to conduct the flow of cash digitally using a three-step process: "Verify Transactions, Protect Requests, and Maintain Historical Records" [21]. This three-step process allows Bitcoin, for the most part, to ensure the integrity and security of transactions throughout the network.

Introduction to Ethereum

Another approach to blockchain is Ethereum, introduced by Vitalik Buterin's 2014 paper, "A next-generation smart contract and decentralized application platform" [32]. Ethereum was developed to address several limitations of Bitcoin, such as the non-flexibility of its scripting language and not being able to hold more complex applications beyond 1 on 1 simple transactions, with slow processing times of adding blocks to the chain. Ethereum's goal is to offer a versatile platform not only for digital currency but also for decentralized applications and smart contracts.

Like Bitcoin, Ethereum is a decentralized network; however, unlike Bitcoin, Ethereum uses a peer-to-peer transactional platform. Its inner mechanics are based on an enhanced digital ledger system, allowing it to support an incredibly wide range of applications beyond merely transferring currency. A public, decentralized record of all the transactions occurring in its ecosystem—that could represent the transfer of Ether (ETH), its native cryptocurrency, but also other complicated data structures like smart contracts—is a main feature of the Ethereum blockchain carried out through the network.

According to Vitalik 2016 [33], the definition of a smart contract is "a computer program that directly controls digital assets". Contracts have their own addresses, and so can serve as owners of digital assets in the same way that users can; if a contract does "own" digital assets, that means that

1. Only the contract's code executing can send the asset to another party, and
2. Every party that sees and can verify the blockchain is aware that the asset is under this program's control.

How Does Ethereum Work?

Users interact with software called "wallets" to execute transactions and deploy smart contracts on the Ethereum network. An Ethereum wallet, much like a Bitcoin wallet, is a digital tool that allows an individual to safely store, send, and receive Ether (ETH). This also manages one's interaction with the Ethereum network regarding the deployment and execution of smart contracts [34]. It has cryptographic keys, just like in Bitcoin wallets, available in both public and private versions, and these serve as the paths to access Ether and smart contracts recorded on the blockchain. A public key is an address others can use to send Ether or interact with smart contracts, while the private key is almost a secret code allowing its wallet owner to control their assets and contract interactions.

Then, upon receiving a smart contract or a request for a transaction, recipient systems authenticate the digital signature against the public key of the sender. That is to say, it verifies the corresponding private key holder has rightfully authorized a transaction or initiation of the contract [35]. Passing through this authentication checkpoint, the requested transaction or contract is then broadcast across an entire Ethereum network for verification of the request by nodes.

A verifying node in the Ethereum network needs to identify two main pieces of information [36]:

1. Sufficient Funds: The node checks that the spender of an amount of ETH (Ethereum's currency) has sufficient funds in their account. All instances of the spending public key on the Ethereum ledger are checked for this, and the exact amount of funds available in the account of the spending party is calculated.

2. Contract Validity: For smart contracts, nodes must verify that the contract code is correctly executed and the conditions specified inside their respective contracts are complied with.

How Does Ethereum Address Its Verification Challenges? Even after a node completes the verification of a requested transaction or contract, the Ethereum network still needs to solve the problem of how to achieve consensus in a decentralized system. Considering that in the Ethereum network, transactions and contract requests are forwarded from node to node, their order of arrival at any given node will not necessarily correspond to their order of creation.

To tackle the challenge of multiple blocks being proposed simultaneously, Ethereum utilizes what is called "proof of stake" (PoS), since the introduction of Ethereum 2.0 (Before this update, the Ethereum platform was using the proof of work mechanism, like Bitcoin). Unlike Bitcoin's proof of work mechanism, which uses enormous computational resources to solve complex mathematical problems, Ethereum's PoS involves a process in which the chance of a validator to propose and validate new blocks is based on the amount of cryptocurrency held by the validator and willing to "stake" as collateral [37].

Validator selection takes place proportionately to stake, and the proposed new blocks are then voted on by the community of the other validators for their validity in order to ensure that the blockchain is secure and consistent.

Benefits of Ethereum

Ethereum offers many potential benefits and future prospects, particularly through its secure technology, flexible and versatile applications, and potential for high returns.

Firstly, Ethereum's secure technology is fundamentally supported by its blockchain infrastructure, which is decentralized and utilizes advanced cryptographic techniques. The security of Ethereum is predominantly maintained through its proof of stake (PoS) mechanism. Unlike the energy-intensive proof of work (PoW) used by Bitcoin, PoS allows for a more efficient and scalable network [38] by selecting validators based on their stake in the system, thereby reducing the risk of centralization and increasing the overall security of the network.

Secondly, Ethereum provides flexible and versatile applications that extend beyond simple financial transactions. Through its support for smart contracts and decentralized applications (dApps), Ethereum enables developers to create and deploy a wide range of innovative applications on its platform. This flexibility allows for the automation of complex agreements, reducing the need for intermediaries and minimizing transaction costs. [39]

Lastly, Ethereum presents significant potential for high investment returns . Its decentralized structure and widespread adoption as a platform for dApps and smart contracts have contributed to its increasing value over time. Historically, Ether, like Bitcoin, has shown substantial price appreciation, attracting investors looking for significant returns. Although the volatility of the cryptocurrency market poses risks, the growing adoption of Ethereum by both developers and institutions suggests that its value may continue to rise, solidifying its position as a key asset in diversified investment portfolios [40].

Ethereum was designed to expand the capabilities of blockchain technology, notably Bitcoin’s technology, beyond simple financial transactions. Created by Vitalik Buterin, Ethereum was introduced as a way to build decentralized applications (dApps) and execute smart contracts on a global scale, while still providing a secure and transparent environment [32]. Ethereum's flexible platform presents a multitude of opportunities across various industries. Using its advanced blockchain architecture, smart contract functionality, and proof of stake (PoS) consensus mechanism [33], Ethereum is able to facilitate complex transactions and applications through a three-step process: Deploy Contracts, Verify Transactions, and Execute Agreements. This three-step process allows Ethereum, for the most part, to ensure the reliability, efficiency, and security of operations throughout the network.

Analysis of Phishing Attacks on Bitcoin and Ethereum

In this section, we will first study in detail phishing attacks on the two major cryptocurrency networks: Bitcoin and Ethereum. These will be compared with respect to the methodologies employed by attackers in both systems. Given

the decentralized nature and differing technologies underlying Bitcoin and Ethereum, it is essential to examine how these differences influence the prevalence and execution of phishing attacks within each ecosystem.

Then, we will discuss the current most common methods of defense against phishing.

Finally we will offer recommendations for enhancing these defenses and provide a recommendation of our own.

Phishing Attacks in Bitcoin

General Statistics and Prevalence of Phishing Attacks

Phishing has remained one of the most widespread attack vectors in the Bitcoin ecosystem. According to a report by Chainalysis in 2021, phishing attacks made up nearly 40% of all cryptocurrency-related scams prone to Bitcoin as the primary target. This highlights the extensive use of phishing in order to fool victims within the Bitcoin network. According to the same report, Bitcoin-related phishing activities peaked during the highly volatile times of cryptocurrency markets, including the 2017 and 2020 bull runs. This was a time when users started making fast profits and became most vulnerable to phishing activities, thus reaching a peak in attacks aimed at credential theft, private key theft, and direct transfer of Bitcoins to the fraudsters' addresses. A study by Kaspersky revealed that almost 20 percent of all phishing emails with the use of cryptocurrencies led to some form of compromise from the cyberattack, either through theft of credentials or the open loss of funds. This shows how effective a phishing campaign is in the cryptocurrency space and also serves to indicate the urgent need for security measures to be heightened so that most users do not fall prey to the attacks. [41] [42]

Financial Losses from Major Phishing Attacks

Quite a few successful phishing attacks have resulted in huge monetary losses for Bitcoin users. One of the largest and most famous attacks targeted a hardware wallet provider called Ledger. The company suffered a massive data breach in 2020 that exposed the personal data of over 270,000 customers, including their email addresses and physical addresses. Phishers took advantage of this information and sent out emails to potential victims that seemed to be from Ledger, which would ask for the user to enter the seed phrases in scam sites. As a result, users lost millions of dollars in Bitcoin, demonstrating how phishing can devastate even those who use hardware wallets, which are generally considered one of the most secure methods of storing cryptocurrency. [43]

Another significant attack occurred in 2015 when a Bitcoin payment service provider, BitPay, lost 5,000 BTC (about $1.8 million) due to a spear phishing attack. In this case, attackers impersonated the BitPay's Chief Financial Officer (CFO) and conned the CEO into authorizing a huge Bitcoin transfer. The sophistication of the phishing scheme highlights the ability of attackers to deceive even experienced professionals within the cryptocurrency industry.

Another significant attack occurred in 2015, when BitPay, a Bitcoin payment service provider, fell victim to a phishing attack that defrauded the company of 5,000 BTC (worth approximately $1.8 million at the time). In this case, attackers impersonated BitPay's Chief Financial Officer (CFO) and tricked the CEO into authorizing a large Bitcoin transfer. The sophistication of the phishing scheme highlights the ability of attackers to deceive even experienced professionals within the cryptocurrency industry. [44]

The Mt. Gox exchange, which collapsed between 2011 and 2014, also saw numerous phishing attempts that contributed to the loss of user funds. Although the takedown of Mt. Gox was mostly attributed to internal theft and poor security practices, phishing attacks added to the chaos and caused further Bitcoin losses for unsuspecting users. In all, Mt. Gox lost 980,000 BTC, which was worth $473 million then, though not all this can be directly attributed to phishing. However, it goes on to show how phishing can exacerbate failures that were already present within cryptocurrency exchanges. [45]

Common Phishing Methods and Their Impact

Email phishing remains one of the more significant threats to the Bitcoin ecosystem. According to Anti-Phishing Working Group (APWG), cryptocurrency-related phishing emails accounted for 12% of total worldwide phishing emails in 2022. Most of those emails were directed at famous Bitcoin exchanges or wallet providers, asking users to log in with their credentials or transfer Bitcoin to addresses that were part of the scam. [46]

Social media was also a very common vector. In many cases, attackers create fake profiles impersonating prominent figures in the cryptocurrency space or support staff from well-known exchanges. These campaigns can be used to get users either to click malicious links or to send Bitcoin to scam addresses. More than 20,000 fake social media accounts were identified in 2021 and 2022, resulting in a potential theft of about 15,000 BTC. The widespread use of social media as a phishing vector demonstrates the need for vigilance when interacting with cryptocurrency-related accounts online. [47]

Notable Phishing Campaigns

Several large-scale phishing campaigns have targeted Bitcoin users with considerable success. One 2021 phishing campaign organized through the use of Google Ads became particularly notorious. Hackers used Google Ads to drive traffic to fake cryptocurrency wallet websites, making them appear at the top of search results. If a user clicked on the advertisement, they were redirected to a phishing website, which posed as a real wallet service. It netted them more than $500,000 in Bitcoin and other cryptocurrency thieves within a few days. [48]

Fake Initial Coin Offerings (ICOs) were another major source of phishing attacks during the 2017-2018 cryptocurrency boom. In this boom, phishers created cloned websites of an ICO that looked exactly like the original site. After that, they convinced people that if they sent a certain amount of Bitcoin to a particular wallet, then they would be rewarded with tokens of a company that did not even exist. More than $2.2 million Bitcoin was lost in this wave of phishing scams, due to the fact that so many investors were interested in this booming ICO market without performing proper background research. [49]

Geographical Distribution and Trends Over Time

Phishing attacks on Bitcoin users are not spread uniformly around the globe. According to a report by CipherTrace in 2020, more than 60% of all reported phishing attacks against Bitcoin users originated from North America and Europe. These areas have significant adoption rates of Bitcoin and other cryptocurrency products; hence, making them the most lucrative regions for phishers. However, the rate of phishing attacks has increased in emerging markets as well. In 2022, there has been a 150% rise in phishing attacks on Bitcoin users over the previous year across Africa and Southeast Asia. This has been attributed to the rapidly growing adoption of Bitcoin across these regions, wherein users might be less aware of safety practices needed to protect their assets. [47]

When the price of Bitcoin skyrockets during bull markets, phishing attacks tend to rise along with it. For example, in 2017, the so-called bull run led to a four-fold increase in phishing activities as new investors joined the markets. The same trend was observed in the 2020 bull market, wherein, with the new all-time highs that Bitcoin's price reached, the phishing attacks doubled. This trend may suggest that the phishers are opportunistic, targeting users when interest in Bitcoin is at its peak. [50]

Phishing Attacks in Ethereum

General Statistics on Phishing in Ethereum

According to Chainalysis, there has been an increase in phishing against Ethereum users. In 2021 alone, phishing constituted almost 50% of all scams against Ethereum. This increase comes with the volume of DeFi activity on the rise and the growing trend in NFTs, which increases the number of susceptible users within the ecosystem. [41]

MetaMask, a widely used Ethereum wallet, has said that there has been a major rise in attackers' success in phishing on their platform [51]. They explained this is likely due to their users' lack of education in preventing these attacks, enabling hackers to gain unauthorized access to decentralized applications and drain them of their assets. While these success rates are apparently not much different from those related to Bitcoin attacks, due to the involved integrations of smart contracts, Ethereum users face special risks linked with using or exploiting these in a manner which creates additional vulnerabilities.

Financial Losses Due to Phishing in Ethereum

Phishing attacks on Ethereum have resulted in significant financial losses over the years. One of the most notable is the 2018 attack whereby the attackers exploited vulnerabilities in DNS to route users into a fake MyEtherWallet (MEW) website. The result was a loss of 215 ETH ($150,000 at the time). What the attackers did was to show the complexity of phishing strategies on Ethereum, from domain hijacking to more complex redirection techniques. [52]

In comparison, Bitcoin has also seen high-profile phishing attacks. In 2020, for instance, scammers breached high-profile accounts,such as the accounts of Elon Musk and Bill Gates, in order to push a fake Bitcoin giveaway scheme that amounted to some $120,000. The hack targeting the Bitcoin community did show an attack that went further than any other nation-state so far in the story of cryptocurrency and just how exposed the community was to phishing. In contrast to the MEW attack that Ethereum faced, which was based on complex DNS vulnerabilities, Twitter hacking was more reliant on social engineering and a failure in the centralized platform's security. [53]

The 2017 ICO boom was another period marked by widespread phishing attacks. Phishing during this time managed to steal about 2.2 million dollars of Bitcoin, with fake ICO websites and phishing emails being the means of stealing the money. Ethereum was used as a launch platform for most of the ICOs, leading Ethereum took the lead in bearing the full force of these phishing campaigns, since many of the ICOs were being conducted on the Ethereum network and users sent ETH instead of BTC to the addresses provided by fraudsters. Thus, even though Bitcoin was the currency involved in these attacks, users of Ethereum were targeted more frequently because the platform was at the center of these scam ICOs. [49]

Common Phishing Methods and Their Impact

Fake wallet websites are among the most prevalent phishing methods in Ethereum. An estimated research study by CipherTrace found that $50 million plus in Ethereum has been lost to fake Ethereum wallet websites by 2021 [54]. These sites frequently pose as popular wallets, like MetaMask or MyEtherWallet, and trick users into typing their private keys or seed phrases, after which the attacker uses them to drain the user's account. This phishing is very similar to techniques used against Bitcoin users, where fake wallet applications and websites are also common. This phishing method is especially disastrous in the case of Ethereum users, however, due to how highly dependent the Ethereum ecosystem is on wallets for interactions with smart contracts and DeFi platforms. The compromise of a wallet can lead to losses way beyond those in funds stored in them, extending to access to various dApps and DeFi accounts.

Another significant problem faced by the Ethereum community is email phishing campaigns. At least 10% of phishing emails worldwide in 2022 were cryptocurrency-related, with most targeting the Ethereum community. In these phishing campaigns, over 50,000 ETH have been stolen [46]. Most of these emails have involved pretending to be official support teams or exchanges in their emails and request sensitive information from people.

Urgent phishing emails, making users believe their accounts are in danger, are fairly common in both Ethereum and Bitcoin; however, because of Ethereum's more complex ecosystem, it can be inferred that Ethereum users have a higher risk of email phishing as phishers could also target specific dApp interactions, adding an additional layer of deception for security measures.

Like Bitcoin, social media phishing has also become one of the major attack vectors against Ethereum users. In 2021 alone, over 46000 users reported over $1 billion dollars in crypto was lost to scams. From this $1 billion dollars, Ether accounted for 9% of it. And again, around 40% of all these scams were said to have originated from

social media. Notable social media applications such as Instagram and Facebook accounted for almost 60% of social media scams, where a number of fake support groups and bots have targeted Ethereum users. This form of phishing, in which messages are sent through impersonation, is similar to the social media scams that affect Bitcoin users. [55]

Notable Phishing Campaigns on Ethereum

One of the most sophisticated phishing campaigns targeting Ethereum users involved the decentralized exchange Uniswap back in 2021. In this campaign, hackers sent phishing emails to Uniswap users, creating fake websites that allowed them to steal upwards of $8 million in Ethereum and ERC-20 tokens [56]. This attack is important in showing that phishers are no longer solely targeting individual users, but also decentralized platforms, finding ways to exploit complex smart contract interactions for fraud. Comparatively, Bitcoin phishing scams traditionally have relied on more low-hanging fruits, such as wallet and exchange impersonations. The openness of Ethereum's dApps, coupled with its smart contracts, opens up a far larger number of attack vectors related to the trust users place in these platforms.

Conclusion of Analysis

By comparison with Bitcoin, in which most of its phishing often deals with direct theft of credentials and funds, Ethereum's ecosystem of smart contracts and its decentralized applications introduce another layer of complexity to be exploited by phishers. This ecosystem structuring difference leads to more complication in phishing scams on Ethereum compared to Bitcoin, while phishing scams in Bitcoin most often focus on simple but efficient scams, like fake wallet interfaces and exchanges.

Current Defense Methods Against Phishing

Currently, exchanges, wallets, and other platforms use an array of defensive methods to counteract phishing. In this section, we will discuss the most prevalent methods used by these platforms.

Two-Factor Authentication (2FA): By requiring a second form of authentication, like a code sent to the user's personal phone number, Two-Factor Authentication adds an extra layer of security to user accounts by blocking unauthorized malicious actor from accessing into a user's account, even if they were able to find out the user's login credentials. 2FA has been proven to reduce the amount of accounts attacked. For example, exchanges such as Coinbase and Binance mandate the use of 2FA when creating an account in order to increase user protection [57].
Anti-Phishing Tools: In order to detect and prevent phishing attacks, wallets and platforms have started to integrate anti-phishing features into their interfaces. For example, Metamask warns users when they attempt to interact with known phishing websites or dApps [58].

Verified Applications: According to a report by Tessian, around 3% of phishing attacks involved users downloading malicious applications or visiting unofficial websites [59]. To help reduce the risk of users interacting with fake wallets and DNS spoofed websites, users are encouraged to download applications only from verified sources, such as official websites or app stores.

Recommendations For Defending Against Phishing

While current defense systems in place have been largely effective against phishing attempts and attacks, there is still much work to be done. As discussed in [Section 4], phishing attacks are still prevalent, leading to massive losses for users. In the section, we will give recommendations that platforms should use to help lower the chances of successful phishing attempts.

Analysis of User Behavior: In order to detect phishing attempts in real time, one can implement behavior analysis tools to monitor user activities for anomalies. By analyzing patterns such as unusually large withdrawals or interactions with unknown smart contracts, a platform using behavior analysis tools will be able to detect suspicious activities

at an early stage. In addition, machine learning algorithms can also prompt users to verify transactions, thus adding additional security to a user's account

Verifying Identities in a Decentralized Manner: In order to verify the authenticity of blockchain addresses and smart contracts, a platform could mandate the use of decentralized identifiers (DIDs). DIDs can help users confirm that they are interacting with legitimate entities. Although the concept of DIDs is not something new, its appliance to counter phishing attacks would require an innovative approach. A system that uses DIDs would let users verify credentials and messages; thus, reducing the risk of users engaging with malicious actors.

Educating users: The best way to fight against phishing lies in the area of user education. Most phishing attacks are built upon social-engineering concepts that mislead users,and statistics reveal that most of the scams happen because of user ignorance of phishing. Through education concerning how to identify phishing attempts and the general tricks used by fraudsters can position the user to recognize these threats and avoid them, thus reducing the overall success rate of phishing attacks.

Conclusion

Phishing remains one of the most prominent threats in blockchain, posing a great risk to financial security across various online networks such as Bitcoin and Ethereum. Attacks of this nature are rampant because they capitalize on social-engineering tropes that can easily trick uneducated users. In this paper, we gave a comparative analysis of phishing on both Bitcoin and Ethereum. We concluded that Ethereum is likely more susceptible to more complex phishing attacks due to its more complex network of decentralized applications and smart contracts. By contrast, the straightforward architecture of Bitcoin has led to more direct attacks, usually on exchanges and wallets. This discussion not only highlighted the complexities of how phishing works on different blockchains, but also gave useful information to users who may have not had this possible risk in mind. Understanding these mechanisms is crucial for anyone involved in cryptocurrency as user awareness is usually the first line of defense against phishing.

Next, we described some existing measures in order to eliminate the threats of phishing. The use of 2FA, anti-phishing inbuilt features within different platforms, and encouraging the use of verified applications have proven to help minimize the number of successful phishing attacks. Such tactics add more layers to defense so that a successful execution of a scheme becomes harder. Lastly we made recommendations that serve to build on present protection strategies including the introduction of user behavior analysis, Decentralized ID authentication solutions, and heavily educating users on how to identify and avoid phishing scams.

In the future, we aim to provide a larger analysis of phishing attacks on Bitcoin and Ethereum in order to deepen our understanding of the pattern and trends of attacks. This can help us develop more effective resources for educating users about phishing attacks and blockchains. By deepening our understanding of patterns and trends of phishing attacks, and by providing users with a high level of education of these dynamics, we can help decrease the success rate of attacks, thus strengthening overall blockchain security.

Acknowledgments

I would like to thank my advisor for the valuable insight provided to me on this topic.

References

[1] Whittaker, C., Ryner, B., & Nazif, M. (2010, February). Large-Scale Automatic Classification of Phishing Pages. In Ndss (Vol. 10, p. 2010).

[2] Khonji, M., Iraqi, Y., & Jones, A. (2013). Phishing detection: a literature survey. IEEE Communications Surveys & Tutorials, 15(4), 2091-2121. https://doi.org/10.1109/SURV.2013.032213.00009

[3] Rekouche, K. (2011). Early phishing. arXiv preprint arXiv:1106.4692.

[4] Weider, D. Y., Nargundkar, S., & Tiruthani, N. (2008, July). A phishing vulnerability analysis of web based systems. In 2008 IEEE Symposium on Computers and Communications (pp. 326-331). IEEE.

[5] Vega, J., Shevchyk, D., & Cheng, Y. (2022). A literature survey of phishing and its countermeasures. In Second Annual Computer Science Conference for CSU Undergraduates.

[6] Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. Communications of the ACM, 50(10), 94-100.

[7] Andryukhin, A. A. (2019, March). Phishing attacks and preventions in blockchain based projects. In 2019 international conference on engineering technologies and computer science (EnT) (pp. 15-19). IEEE.

[8] Kirby, J. (2020, January 21). The Saudi crown prince reportedly hacked Jeff Bezos. Vox. https://www.vox.com/2020/1/21/21075990/saudi-arabia-crown-pince-mbs-amazon-jeff-bezos

[9] Gordover, M. (2015, March 26). Throwback Hack: The Epsilon Email Breach of 2011 [Review of Throwback Hack: The Epsilon Email Breach of 2011]. Proofpoint. https://www.proofpoint.com/us/blog/insider-threat-management/throwback-hack-epsilon-email-breach-2011

[10] 2018 Cryptocurrency Exchanges. User Accounts Leaks Analysis. (2018). Group-Ib.com. https://go.group-ib.com/report-cryptocurrency-exchanges-en?_gl=1’

[11] Sarmah, S. S. (2018). Understanding blockchain technology. Computer Science and Engineering, 8(2), 23-29.

[12] Ismail, L., & Materwala, H. (2019). A review of blockchain architecture and consensus protocols: Use cases, challenges, and solutions. Symmetry, 11(10), 1198. https://doi.org/10.3390/sym11101198

[13] Miakish, N. (2023, April 13). Decoding the Fundamentals of Blockchain Architecture. SumatoSoft. https://sumatosoft.com/blog/decoding-the-fundamentals-of-blockchain-architEcture-a-comprehensive-guide.

[14] Deshpande, V., Badis, H., & George, L. (2022). Efficient topology control of blockchain peer to peer network based on SDN paradigm. Peer-to-Peer Networking and Applications, 15(1), 267-289.

[15] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Satoshi Nakamoto.

[16] Hillary, & Scott-Briggs, A. (2024, August 16). Blockchain Architecture: Creating Scalable and Reliable Blockchain Networks. TechBullion. https://techbullion.com/blockchain-architecture-creating-scalable-and-reliable-blockchain-networks/

[17] Cha, J., Singh, S. K., Pan, Y., & Park, J. H. (2020). Blockchain-based cyber threat intelligence system architecture for sustainable computing. Sustainability, 12(16), 6401.

[18] Blockchain and the environment. (2020). European Environment Agency. https://www.eea.europa.eu/publications/blockchain-and-the-environment#additional-files.

[19] Arti Damale. (2024, August 27). Layer-2 Solutions vs. Sharding: Which is the Better Scalability Solution? SDLC Corp. https://sdlccorp.com/post/layer-2-solutions-vs-sharding-which-is-the-better-scalability-solution/

[20] Notomoro. (2024, February 13). 16 Disadvantages of Blockchain: Limitations and Challenges - Webisoft Blog. Webisoft. https://webisoft.com/articles/disadvantages-of-blockchain/

[21] Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. Applied innovation, 2(6-10), 71.

[22] Vujičić, D., Jagodić, D., & Ranđić, S. (2018, March). Blockchain technology, bitcoin, and Ethereum: A brief overview. In 2018 17th international symposium infoteh-jahorina (infoteh) (pp. 1-6). IEEE. https://doi.org/10.1109/INFOTEH.2018.8345547

[23] What Is a Bitcoin Wallet? (2024, August 29). Cryptonews.net. https://cryptonews.net/editorial/guides/what-is-a-bitcoin-wallet/

[24] Volety, T., Saini, S., McGhin, T., Liu, C. Z., & Choo, K. K. R. (2019). Cracking Bitcoin wallets: I want what you have in the wallets. Future Generation Computer Systems, 91, 136-143.

[25] Rodeck, D. (2023, May 23). What Is Blockchain? Forbes Advisor. https://www.forbes.com/advisor/investing/cryptocurrency/what-is-blockchain/

[26] Sinkevicius, A. (2022, June 5). How do Bitcoin nodes validate transactions in blockchain? Coinmonks. https://medium.com/coinmonks/how-do-bitcoin-nodes-validate-transactions-in-blockchain-7ec0603a0140

[27] Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D., ... & Peacock, A. (2019). Blockchain technology in the energy sector: A systematic review of challenges and opportunities. Renewable and sustainable energy reviews, 100, 143-174.

[28] Tschorsch, F., & Scheuermann, B. (2016). Bitcoin and beyond: A technical survey on decentralized digital currencies. IEEE Communications Surveys & Tutorials, 18(3), 2084-2123.

[29] Fauzi, M. A., Paiman, N., & Othman, Z. (2020). Bitcoin and cryptocurrency: Challenges, opportunities and future works. The Journal of Asian Finance, Economics and Business, 7(8), 695-704.

[30] Bariviera, A. F., Basgall, M. J., Hasperué, W., & Naiouf, M. (2017). Some stylized facts of the Bitcoin market. Physica A: Statistical Mechanics and its Applications, 484, 82-90.

[31] Biggs, N. A., Hoa Nguyen and John. (2022, Aug 5). Why Use Bitcoin? Www.coindesk.com. https://www.coindesk.com/learn/why-use-bitcoin/

[32] Buterin, V. (2014). A next-generation smart contract and decentralized application platform. white paper, 3(37), 2-1.

[33] Buterin, V. (2016). Ethereum: platform review. Opportunities and challenges for private and consortium blockchains, 45, 1-45.

[34] Lee, B. J. P., & Product, C. P. M. K. D. D. of D. A. (n.d.). Smart Contract and Ethereum Explained: FAQ | VanEck. Smart Contract and Ethereum Explained: FAQ | VanEck. https://www.vaneck.com/us/en/blogs/digital-assets/smart-contract-and-ethereum-explained-faq/

[35] Ethereum, in. (2018, February 17). Signing and Verifying Messages in Ethereum. Programtheblockchain.com. https://programtheblockchain.com/posts/2018/02/17/signing-and-verifying-messages-in-ethereum/

[36] An overview of how smart contracts work on Ethereum | QuickNode. (2024, Sept. 17). Www.quicknode.com. https://www.quicknode.com/guides/ethereum-development/smart-contracts/an-overview-of-how-smart-contracts-work-on-ethereum

[37] Nguyen, C. T., Hoang, D. T., Nguyen, D. N., Niyato, D., Nguyen, H. T., & Dutkiewicz, E. (2019). Proof-of-stake consensus mechanisms for future blockchain networks: fundamentals, applications and opportunities. IEEE access, 7, 85727-85745. https://doi.org/10.1109/ACCESS.2019.2925010

[38] King, S., & Nadal, S. (2012). Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. self-published paper, August, 19(1).

[39] What is a smart contract, and how does it work? (2024, August 28). Cointelegraph. https://cointelegraph.com/learn/what-are-smart-contracts-a-beginners-guide-to-automated-agreements
[40] VanEck. (2024, June 4). The Investment Case For Ethereum In 2024. Seeking Alpha. https://seekingalpha.com/article/4697303-ethereum-investment-case-2024

[41] Chainalysis. (2021). The Chainalysis 2021 crypto crime report. Go.chainalysis.com. https://go.chainalysis.com/2021-Crypto-Crime-Report.html

[42] Kaspersky Security Bulletin 2021. Statistics. (2021). https://go.kaspersky.com/rs/802-IJN-240/images/KSB_statistics_2021_eng.pdf

[43] Message by LEDGER's CEO - Update on the July data breach. Despite the leak, your crypto assets are safe. (2020, December 21). Ledger. https://www.ledger.com/message-ledgers-ceo-data-leak

[44] Stu Sjouwerman. (2015, September 19). BitPay loses 1.8 Million In Phishing Attack. Knowbe4.com; KnowBe4, Inc. https://blog.knowbe4.com/bitpay-loses-1.8-million-in-phishing-attack

[45] Harney, A., & Stecklow, S. (2017, November 17). Special Report: Twice burned - How Mt. Gox's bitcoin customers could lose again Reuters. https://www.reuters.com/article/technology/special-report-twice-burned-how-mt-goxs-bitcoin-customers-could-lose-again-idUSKBN1DG1UA/

[46] APWG (2022). Phishing Activity Trends Report, 3rd Quarter 2022. APWG. https://docs.apwg.org/reports/apwg_trends_report_q3_2022.pdf#:~:text=Phishing%20Activity%20Trends%20Report,%203rd%20Quarter%202022%20APWG%20member%20Agari

[47] Cryptocurrency crime and anti-money laundering REPORT. (2022). https://info.ciphertrace.com/hubfs/CAML%20Reports/CipherTrace%20Cryptocurrency%20Crime%20and%20Anti-Money%20Laundering%20Report%2c%20October%202022.pdf

[48] Check Point Research Team. (2021, November 4). Scammers used Google Ads to Steal ~ $500k Worth of Cryptocurrency https://blog.checkpoint.com/security/scammers-used-google-ads-to-steal-500k-worth-of-cryptocurrency/

[49] Cointelegraph. (2024, April 2). History of Crypto: The ICO Boom and Ethereum's Evolution. Cointelegraph. https://cointelegraph.com/news/ethereum-ico-boom-history-crypto

[50] Cryptocurrency Crime and Anti-Money Laundering Report, Spring 2020. (2020). Docslib. https://docslib.org/doc/7189012/cryptocurrency-crime-and-anti-money-laundering-report-spring-2020.

[51] How and Why are MetaMask Users Losing their Funds due to Phishing Incidents? | Consensys. (2022). Consensys. https://consensys.io/blog/how-and-why-are-metamask-users-losing-their-funds-due-to-phishing-incidents

[52] Floyd, D. (2018, April 24). $150K Stolen From MyEtherWallet Users in DNS Server Hijacking. Yahoo Finance; Yahoo Finance. https://finance.yahoo.com/news/150k-stolen-myetherwallet-users-dns-163521584.html

[53] Team, C. (2020, July 22). The Twitter Hack: What We Know One Week Later - Chainalysis. Chainalysis. https://www.chainalysis.com/blog/twitter-hack-july-2020-update/

[54] Cryptocurrency Crime and Anti-Money Laundering Report CipherTrace Cryptocurrency Intelligence. (2021). https://info.ciphertrace.com/hubfs/CAML%20Reports/CipherTrace%20Cryptocurrency%20Crime%20and%20Anti-Money%20Laundering%20Report%20-%20May%202021.pdf

[55] Fletcher, E. (2022, June 3). Reports show scammers cashing in on crypto craze. Federal Trade Commission. https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/06/reports-show-scammers-cashing-crypto-craze

[56] The 2021 Crypto Crime Report Everything you need to know about ransomware, darknet markets, and more. (2021). https://go.chainalysis.com/rs/503-FAP-074/images/Chainalysis-Crypto-Crime-2021.pdf

[57] Rosencrance, L. (2021, July). What is two-factor authentication (2FA) and how does it work? TechTarget. https://www.techtarget.com/searchsecurity/definition/two-factor-authentication

[58] Young, M. (2021, May 3). MetaMask warns of new phishing bot. Cointelegraph. https://cointelegraph.com/news/metamask-warns-of-new-phishing-bot

[59] Rosenthal, M. (2022, January 12). Must-Know Phishing Statistics: Updated 2020. Tessian; Tessian. https://www.tessian.com/blog/phishing-statistics-2020/