National College of Ireland

Decentralized Solution to Mitigate Job Posting Scams by Proving Ownership and Identity

MSc Research Project
Cloud Computing

Apostolos Giannakidis
Student ID: x20124066

School of Computing
National College of Ireland

Supervisor: Horacio Gonzalez-Velez

National College of Ireland
Project Submission Sheet
School of Computing

Student Name:	Apostolos Giannakidis
Student ID:	x20124066
Programme:	Cloud Computing
Year:	2021-22
Module:	MSc Research Project
Supervisor:	Horacio Gonzalez-Velez
Submission Due Date:	15/Aug/2022
Project Title:	Decentralized Solution to Mitigate Job Posting Scams by Proving Ownership and Identity
Word Count:	9621
Page Count:	25

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature:	Apostolos Giannakidis
Date:	15th August 2022

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST:

Attach a completed copy of this sheet to each project (including multiple copies).	☐
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	☐
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	☐

Assignments that are submitted to the Programme Coordinator office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

This research is dedicated to Afroditi, my soon-to-be wife.

Acknowledgements

First of all, I would like to thank my supervisor Horacio Gonzalez-Velez for his dedicated support, thoughtful comments and guidance on this dissertation.

Special thanks to my family and friends for all the unconditional support and encouragement during this very intense academic and professional year of my life. Specifically, to my parents Dionisia, Anastasios, my brother Marinos, my soon-to-be wife Afroditi and my friends Panagiotis Yialouris, Theodore Chaikalis, Thomas Pelioglou, and Chris Tognini.

Additionally, I would like to express my gratitude to my colleagues at Microsoft, specifically Thomas Maher, Christer Ljung, Daniel Godbout and Rohit Gulati. This project would not have been the same without their guidance.

Finally, I would like thank the Springboard programme that partially funded this postgraduate course.

We live in a society exquisitely
dependent on science and technology,
in which hardly anyone knows anything
about science and technology.

CARL SAGAN

Decentralized Solution to Mitigate Job Posting Scams by Proving Ownership and Identity

Apostolos Giannakidis
x20124066

Abstract

In a recent public announcement, the FBI warned the public about a scam scheme on career-oriented social networking platforms. Scammers exploit security vulnerabilities on these platforms that allow them to post fraudulent job advertisements in an attempt to trick unsuspecting applicants, who are unable to verify the identity of the job poster, to submit their personal information. Victims are financially damaged and impersonated organizations are reputationally affected. This research is proposing a decentralized system using Blockchain, public Cloud and decentralized services as a mitigation control against this scam. This novel solution uses Non-Fungible Tokens (NFT) to verify the ownership of job posts and Self-Sovereign Identity (SSI) / Decentralized Identifiers (DID) to verify the identity and provide authorization to job posters. To evaluate its feasibility and the research results, a Proof-of-Concept solution has been developed that runs on the Polygon network on the Ethereum Blockchain and uses Microsoft's Verifiable Credentials Azure service. The delivered Proof-of-Concept proved that it is feasible to mitigate this scam with 100% accuracy for the job posts that have been minted as NFTs.

1 Introduction

Social media platforms provide scammers with new attack vectors to exploit in order to trick users and steal their personal information; a scam also known as *identity theft* [1]. The motivation for this research is the identity theft scam scheme that was disclosed by the Federal Bureau of Investigation (FBI) in a public service announcement on February 01, 2022[1]. The announcement described a new identity fraud scam that has been observed since early 2019 and exploits security issues of multiple career-related social platforms such as the lack strong identity verification controls. Scammers exploit these flaws to post fraudulent job advertisements that are presented alongside legitimate jobs posted by the business. The scam works because the job posts appear authentic and legitimate making it difficult for applicants and the spoofed company to determine which job posting is real and which one is fraudulent. Victims trust these fraudulent job advertisements and submit their personal information and CVs. Scammers then steal the victim's identities and make financial transactions. Each victim is assessed to have on average $3,000 stolen from their bank accounts and have had their credit scores negatively affected.

In the past few months, an extensive research has been conducted to investigate possible solutions to this problem. All researches on the domain aim to solve this problem

[1] https://www.ic3.gov/Media/Y2022/PSA220201

using Machine Learning models with varying levels of accuracy. However, none of them has the ability to determine the legitimacy of the owner of a job post with 100% accuracy. None of these researches is based on a deterministic model and all of them have limiting factors with language being the most important one. This research takes a different approach and investigated whether a decentralized solution based on Blockchain and Self-Sovereign Identity can provide the security guarantees required to protect job applicants and hiring companies against the online job posting scam.

Blockchain serves as a decentralized, cryptographically-strong, digital ledger. Ethereum [2] was the first Blockchain platform that provided support for Smart Contracts, which is code that runs on the Blockchain that enables decentralized parties to conduct fair exchanges without a trusted third party. Non-fungible tokens (NFT) are unique tokens on the Blockchain that represent ownership of unique items. NFTs are digitally unique with unique characteristics. No two NFTs are the same. The process of recording on the Blockchain a digital asset as an NFT is called "minting". Every NFT has an owner that is represented by a Blockchain address, which is a unique alphanumeric sequence of a specific access point on the Blockchain network. The owner's address of an NFT is visible on the public Blockchain ledger and it is easy for anyone to verify. Decentralized applications (dApps) run on Blockchain, powered by Smart Contracts, operate autonomously and are not controlled by a specific entity; a characteristic that gives to these application their decentralized nature [3]. To interact with the Blockchain, users require digital wallets. The wallets store the user's Blockchain private and public keys and allow them to make transactions. The wallet's address is a hash of its public key. The most popular Blockchain wallet is MetaMask that is accessed via a browser extension.

Self-Sovereign Identity (SSI) is an emerging identity management model, that became a popular research topic after the introduction of Blockchain. SSI allows users create and have full control their own identity data, without relying on any centralised authority [4]. Using SSI, users (individuals or organizations) can present their trusted credentials to third parties without having to engage an intermediary party or a central authority. Blockchain-based SSI is based on the Verifiable Credential (VC) [5] and Decentralized IDentifier (DID) [6] W3C standards. Decentralized Identifiers (DIDs) are a new type of digital identifiers that are used to achieve verifiable, "self-sovereign" digital identities that do not depend on any central identity registry or authority. DIDs are URIs that map an individual or an entity (DID subject) a DID document, which is a JSON-LD object that contains public information about the identity, such as public keys, and references to the issuer's repository for Verifiable Credentials (VCs) [7]. Verifiable Credentials are cryptographically secure, privacy respecting, and machine-verifiable digital credentials. Verifiable Credentials represent digital statements about person's identity made and cryptographically signed by an issuer in a tamper-evident manner. VCs can represent digitally physical credentials, such as employee identification cards, driver's licenses, passports or diplomas. They are named Verifiable Credentials due to the characteristic of the credential being able to be verified by external verifiers, without having to rely on requesting verification from the issuer. Verifiable Credentials are stored in digital wallets, typically on the mobile phone of the user. To access the VCs a biometric access control is frequently used. With this model, DIDs and VCs can achieve true identity verification.

Identity Federation is a secure way for third-party applications to get access to a user's identity information [8]. Identity Federation is used to authenticate and authorize users against a trusted Identity Provider (IdP). This way, applications do not have to implement and handle the identity and credential management of each user. With

Identity Federation, applications do not verify the user's identity. Instead, these critical functionalities are delegated to an external IdP that the user already trusts and has an account on. Upon authentication, the user's identity data is sent (federated) back to the application that initiated the authentication process. Using the user's identity data, the application is only responsible for making authorization decisions. To achieve Identity Federation, applications must establish a trust relationship with the third-party IdP.

1.1 Research Question

This research aims to investigate whether a Cloud-based and Decentralized-based system that integrates with popular career platforms can address the online job posting scam. In particular, can the online job posting scam can be addressed via a secure solution that is synthesized from decentralized technologies, specifically Blockchain, Decentralized Identifiers (DIDs), Verifiable Credentials (VCs) and dApps?

1.2 Benefits of this research

The primary stakeholders that would benefit from this solution are the job applicants, who are financially impacted by this scam. Considering that each victim of this scam had on average US$3,000 stolen from their bank accounts, we can estimate that this solution could help the industry save tens of thousands of US dollars. Secondary stakeholders are the career-oriented platforms and the hiring companies whose reputation is negatively impacted. Also, the success of this project could become the basis for protecting other types of digital assets against similar scams. This is because conceptually, this solution is applicable to any other digital asset. Eventually, a successful outcome of this research could benefit the social platform industry and could have the potential of reducing the rate of identity thefts via fraudulent digital content.

2 Related Work

2.1 Research on the Job Scam

To date, most significant studies on the research topic of detecting fraudulent job ads are based on Machine Learning (ML) methodologies. The first public dataset with real-life job ads was created by Vidros et al. [9]. The researchers use the new dataset to experiment and establish a preliminary list of empirical rules for detecting fake job ads. The same researchers continued their work in Vidros et al. [10] where they provide an analysis of the scam's characteristics and its impact. The authors argue that the automatic detection and mitigation of the scam was at the time a largely unexplored domain. In their paper, the authors suggest that detecting the scam by reviewing only the content of job ads often proves to be insufficient. For example, sentiment analysis is ineffective because the content of job ads is usually written in neutral language. For this reason, the authors attempted to address the detection via text mining with metadata. Interestingly, the dataset that Vidros et al. [9] have created has been used in many other studies by other researchers who investigated the same research topic of detecting fake job ads using ML.

Building on the work conducted by Vidros et al. [10], the study from Mahbub and Pardede [11] increased the detector's accuracy up to 97% by enriching the ruleset of the original study with contextual features about the organization that posts the job ad. The main limitation of their work is the manual extraction of the contextual features

and the manual validation process for the output of the name extraction algorithm. A new dataset, created by Nindyati and Nugraha [12], further increased the accuracy of the detector by applying behavioral context-based features. The new dataset contains data obtained from job ads in Indonesia. According to the research, the proposed ML system reached 90% in accuracy, precision and recall. A critical open question is whether the system can work effectively with data, companies and platforms outside of Indonesia.

In Habiba et al. [13], researchers used text mining techniques, however, they proposed a Deep Neural Network (DNN) that uses *Naive Bayes* and *Random Forest* classifiers, and the KNN classification algorithm. The average accuracy of the trained classifier reached an impressive 98%. The authors Keerthana et al. [14], proposed feature engineering techniques like *one-hot encoding*, *TFIDF Vectorizer*, and *count Vectorizer*. The research experiments with multiple prediction algorithms, many of which are not novel in the domain, and the best accuracy they achieved was 71% using the *MLPClassifier*. It can be seen that this research does not achieve better results than previous studies.

In another recent study, Anita et al. [15] achieved accuracy up to 98% by using very similar Machine Learning techniques and methodologies to train a *Bidirectional-LSTM model*. Their research work achieved the highest accurate result in the field.

2.2 Blockchain Solutions on Ownership and Fraudulent Content

The study by Fraga-Lamas and Fernández-Caramés [16] provides a comprehensive overview on the applicability of Blockchain and distributed ledger technologies (DLTs) to tackle digital deception on the Internet and social media. The research reviews several areas of applicability including the decentralized content moderation, trustworthiness of content, fact-checking, decentralized social media platforms (dApps), traceability and tracking services. The research concludes that DLTs provide the necessary trust mechanisms to adequately ensure the authenticity of digital assets while maintaining auditing and accountability for each transaction. The study underscores the importance of having a system that is resilient to falsification attacks by ensuring the integrity of digital assets.

Although this research proposal focuses on the jobs scam, it aligns with the work conducted by Qayyum et al. [17]. In that study, the researchers proposed a Blockchain-based system that addresses the problem of fake news. The proposed system leverages Smart Contracts for the registration of publishers, as well as for the publishing of news items and the maintenance of their integrity. The system works by allowing news publishers to register and be given a key pair (public and private). After a verification process that utilises the key pair, publishers are able to publish news on the network. The system maintains a reputation score for measuring the credibility of each publisher. The integrity of each news item and its truthfulness is verified using a semantic similarity and Merkle tree approach. Note that this study addresses the research question in a theoretical context and no working prototype was created.

In a similar study on the problem of fake news, Chen et al. [18] proposes a Blockchain-based solution that uses a custom Proof-of-Authority (PoA) consensus algorithm and a dynamic weighted-ranking system based on credibility scores that favours news publishers who produce legitimate news compared to the ones that publish fake news. This gamification component acts as an incentive mechanism and creates a hierarchy based on each participant's credibility score. Each participant of the system can validate the news article published by the other participants of the system, based on their credibility score. These participants are called *validators* and they are running the PoA consensus algorithm. Only the news articles marked as legitimate are shown to the public. To prove

their proposal, the researchers developed a Proof-of-Concept (PoC) solution, although their PoC implementation is not publicly available to review.

Regarding the applicability of using Blockchain on social media, the study by Freni et al. [19] reviews the current state of most popular social media and presents evidence that users lose ownership of the content they upload on these social media platforms. On the other hand, systems built with Blockchain always provide the means to continually track and monitor the sharing of uploaded content, while retaining the ownership of the content to the original user.

A study that experimented with Blockchain-based content network was performed by Tee and Murugesan [20]. The researchers proposed a simulation of a Blockchain-based social media platform coupled with an AI algorithm. The study states that such a network is trustable and verifiable and capable of preventing and detecting fake news. Although the study provides many examples of trusted social media platforms backed by Blockchain, the results of the simulations have not been published.

The paper by Qureshi and Megías Jiménez [21] provides a comprehensive survey of Blockchain-based copyright protection systems. According to the researchers, Blockchain is considered to be a reliable solution to address problems related to copyright protection of digital content, digital rights management, data integrity, authenticity and piracy tracing. As stated in the study performed by Jiang et al. [22], Blockchain solves these problems due to its intrinsic ability for traceability, immutability, and transparency. Blockchain is also cost-effective in copyright protection compared to traditional systems.

The proposed solution by Zhaofeng et al. [23] addresses artwork image digital rights using a novel DRM scheme on a Blockchain-based platform called DRMChain. The system creates a watermark with copyright information and embeds it into the image using the *Arnold* transform encryption. The experiment results indicate that the system is trusted and can protect against the misuse of digital data. In a similar research topic, Zhao and O'Mahony [24] proposed a Blockchain-based system, called BMCProtector, that aims to protect digital music copyright and ensure the owners' income rights. Similarly to DRMChain, BMCProtector uses encryption and watermarking to embed copyright data into the digital media as well as to track the propagation path of illegal data sharing.

Finally, with regards to preventing phishing, Liu et al. [25] propose a novel Blockchain-based phishing data sharing mechanism. The researchers designed a theoretical solution on Hyperledger Fabric. According to the study, in order for their proposal to be effective, the participants on their Blockchain must be highly reputable institutions.

2.3 Critique and Identified Gaps

By reviewing the above-mentioned ML studies it is evident that none of these studies is able to detect fraudulent job ads posted by legitimate company accounts that have been hacked. Another problem with the ML detectors is that they are based exclusively on the text of the job posts and highly depended on the job post's language. Effectively, these detectors are capable of detecting fraudulent job posts only in the language that they have been trained for. Thus, they cannot be used to address the job scam for languages and countries for which there is no large data set that can be used to train these ML models. It is also argued that the accuracy of the above-mentioned Machine Learning solutions could be impacted by overfitting errors due to the single available, small, training dataset that contained less than 5% of fraudulent job ads.

On the other hand, the literature review showed how Blockchain can be a trusted solution to trace digital asset ownership in a decentralized network, and how Decentralized

Identifiers can be used to prove a user's identity in a decentralized network. Importantly, there is no identified research study that uses these technologies to combat the scam of fake online jobs. The novelty of this research study is that instead of verifying a job post by analysing its text, it protects job applicants from falling victims to identity theft via fraudulent job posts by using decentralized technologies to prove the ownership of the job post and the identity of the job poster.

3 Methodology

The research methodology chosen to systematically answer the Research Question involves designing and implementing a Proof-of-Concept (PoC) solution. This PoC will be used to demonstrate the feasibility of the proposed concept. This section provides details on the methodology and the steps followed during the delivery of the PoC solution, called *AdvertChain*. It also provides an overview the ethical considerations of this research.

Although the PoC solution focuses on mitigating the job scam by proving their ownership and identity of the job poster, the same approach can be reused for other types of digital assets. Thus, special consideration was given not to restrict the solution in protecting only job posts but to allow the solution to be extended for other types of digital assets in the future with little development effort.

As a research project there is a big element of uncertainty and unknown factors. Therefore, a waterfall methodology (a series of sequential tasks) is not a good choice as it often causes messy results [26]. Instead, this project adopted an iterative approach that allows rapid prototyping. This way, hypotheses can be easily validated and refined quickly. The Software Development Life Cycle (SDLC) of the *AdvertChain* PoC consisted of the following main phases:

1. the analysis and requirements phase
2. the design phase
3. the integration with the social platform (LinkedIn)
4. the implementation phase of the fake company
5. the implementation phase of the Verifiable Credentials Cloud service
6. the implementation phase of the Verifiable Credentials issuer
7. the implementation phase of the Smart Contract
8. the implementation phase of the NFT minter and verifier
9. the test & validation phase
10. the deployment phase
11. the evaluation phase

Each phase had multiple iterations and the implementation followed the Test-Driven-Development methodology. The solution was deployed on a public Cloud to demonstrate its functionality, test the design requirements and evaluate the research objectives.

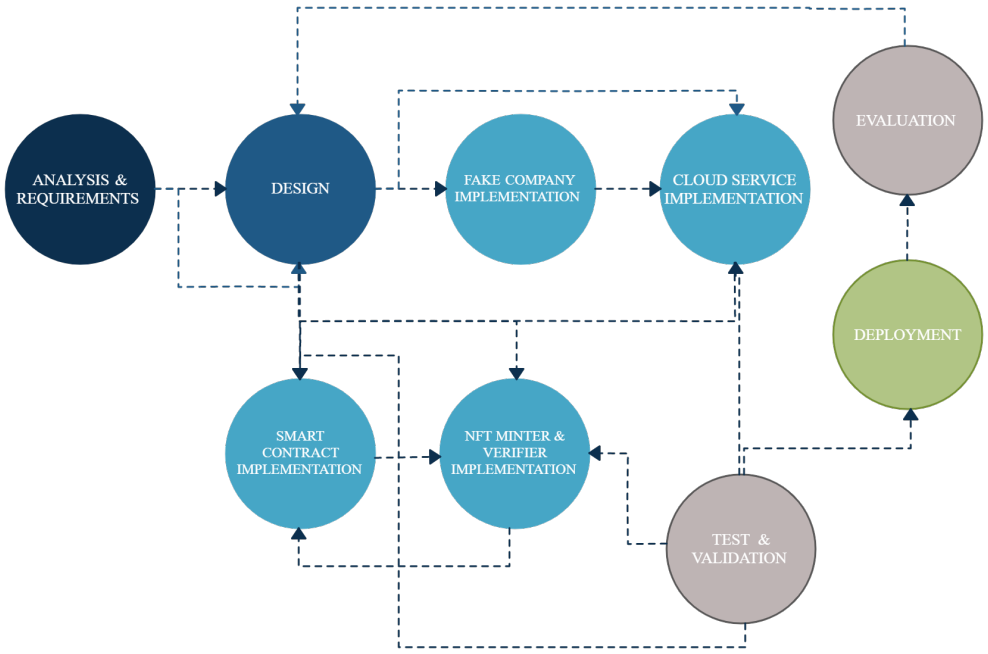

Figure 1: SDLC phases of the *AdvertChain* Proof-of-Concept

3.1 Ethical Considerations

This research project aims to validate the ownership of the job post and identity of the job poster. To achieve its goals, no Personally identifiable information (PII) or other sensitive data are stored. The only handling of PII are the claims contained in the Verifiable Credentials of the job posters. However, job posters explicitly give their consent to *AdvertChain* to retrieve these PII. Also, the retrieved PII are not stored persistently and they only remain in memory of the user's client-side browser. For the evaluation of this research project, no human participants are required nor any datasets with sensitive data. For the development and testing of the PoC implementation of *AdvertChain* only test/mock data and publicly available data were used. In case in the future the proposed solution gets adopted by the career-networking platforms, then only public and globally accessible data will be used. Thus, there are neither anticipated ethical risks, nor any applicable data protection regulations. Having said that, the solution was designed with privacy in mind to eliminate any privacy or ethical risks.

4 Design

The primary goal of the *AdvertChain* Proof-of-Concept (PoC) solution is to protect job applicants from falling victims to identity theft via online fraudulent job posts. Unlike the ML-based solutions that depend on analysing the text of the job posts, the way this solution achieves its goal is by proving the following:

1. the identity of the hiring company is verified
2. the identity of the job poster is verified
3. the job poster is authorized by the hiring company to post job advertisements
4. the job post is authentic (it is actually owned by the verified hiring company)

Note that in this context, the job poster is considered to be an employee working for the hiring company whose role in the company authorizes him/her to post online job ads.

Using NFTs it is possible to cryptographically prove the authenticity and ownership of each job post. However, NFTs can only verify the Blockchain address of the owner and does not prove the identity of the hiring company or the job poster. To verify the identity of the hiring company and the identity of the job poster, this solution uses Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs). To verify the job poster's role and authorization level, a combination of Decentralized Identifiers (DIDs)/Verifiable Credentials (VCs) and Identity Federation is used.

In order to create an end-to-end PoC solution that can be demonstrated, a fake company is also needed that will be used as the hiring company. To this end, a website is needed that is hosted on a public domain as well as a company profile on the career social network. The website is used not only as the company's page but it also hosts the company's DID document as well as the company's Verifiable Credentials issuer web app.

The main two modules of the solution are the NFT minter web app that job posters use to mint new NFTs and the job post verifier that job applicants use to verify job posts.

4.1 Considerations and Decisions Made

During the design and the implementation of this PoC solution, several cases were encountered that required consideration and specific decisions had to be taken. Specifically:

1. Ethereum was chosen as the Blockchain for the *AdvertChain* Smart Contract. Ethereum is currently the most popular Blockchain for NFTs. The platform and tooling has matured and there is a plethora of technical guidance on how to implement NFTs for Ethereum. Additionally, the Polygon layer-2 network was used that allows cost-efficient minting of NFTs and better compatibility with OpenSea.
2. There is no cost to the user for minting *AdvertChain* NFTs. This is because making profit is not a current goal for this PoC solution. This way it will be easier to increase adoption. Note that the NFTs are not meant to be collectibles or to be traded.
3. The Alchemy platform was chosen as the Web3 API client in order to integrate with the Polygon network.
4. The Mumbai Polygon testnet was chosen, as it is the most popular Polygon testnet.
5. To reduce the cost of Ethereum transactions, the NFT metadata must be stored off-chain, on InterPlanetary File System (IPFS). The Pinata Cloud platform was chosen as the way to integrate with IPFS.
6. Microsoft's Azure Active Directory Verifiable Credentials (recently renamed to Microsoft Entra Verified ID) was chosen as the DID/VC service. This is because Microsoft's service is the only DID/VC service offered by a top-tier public Cloud provider with a mature implementation of the W3C standard. The DID method chosen is Identity Overlay Network (ION), which is a Layer 2, open and permissionless network that runs on top of Bitcoin. ION was launched by Microsoft and it is used to store the DIDs and the public signing keys.
7. Microsoft's Azure App Service was chosen to be used as the hosting web service for the fake company's website. This is because it is one of the easiest ways to deploy apps to the Cloud and for our requirements, hosting is virtually free.

8. Google's Firebase was chosen as the platform to deploy the *AdvertChain* NFT minter. This is because Firebase offers a very easy way to deploy apps, to spin up backend services (serverless and databases), a seamless integration with React apps and automated provisioning of free TLS certificates. Additionally, by having a multi-cloud solution, better agility is achieved and vendor lock-in is avoided.
9. LinkedIn was chosen as the career social networking platform because it is currently the most popular platform of its type. Proving the value of this solution using LinkedIn will have bigger impact and it will reach a larger user base. Also, LinkedIn supports Identity Federation by acting as a trusted social Identity Provider (IdP), which is required for this solution.
10. To programmatically retrieve a screenshot of the LinkedIn job post, the NoCodeAPI platform was chosen due to its simple API and its low cost.
11. Tampermonkey was chosen as the way to modify the Document Object Model (DOM) of the job post on LinkedIn. This way the user experience becomes as simple as possible due to the automation of the job post verification. This is an optional component of the PoC that improves the overall user experience and satisfaction.

For this solution to work, it is assumed that the hiring company issues Verifiable Credentials to their employees with specific claims required by *AdvertChain*, every job poster is holder of a VC issued by the hiring company and that every job poster has a valid LinkedIn account and a MetaMask wallet. To enable the end-to-end demonstration of this PoC, a VC issuer was implemented for the fake company.

4.2 Specification

Following are the Functional Requirements of the *AdvertChain* PoC solution:

FR-1 The NFT minter must authenticate users via LinkedIn identity federation.

FR-2 The NFT minter must verify user's identity via a Verifiable Credentials QR code.

FR-3 The NFT minter must allow users to connect their MetaMask wallets.

FR-4 The NFT minter must allow users to type the URL to the LinkedIn job post.

FR-5 Users must be authorized to mint NFTs if all the following conditions are true:

(a) the LinkedIn full name must match the full name from the Verifiable Credential
(b) the LinkedIn user email must match the email contained in the VC claims
(c) the user's VC job role claim must be either Recruiter or Hiring Manager.
(d) the user's VC must be issued by the company that posted the LinkedIn job.
(e) the user's VC issuer must have a verified domain.

FR-6 The NFT Smart Contract must follow the ERC-721 standard.

FR-7 The NFT must not allow to be traded or change ownership after it is minted.

FR-8 The NFT must only be allowed to be minted by the Smart Contract creator.

FR-9 No duplicate NFTs for the same job post must be allowed.

FR-10 The minted NFT's tokenURI parameter must resolve to a JSON document describing the NFT's metadata.

FR-11 For each minted NFT a screenshot must be taken that shows the job post as rendered by LinkedIn.

FR-12 Both the metadata JSON document and the screenshot must be stored on IPFS.

FR-13 The NFT metadata must be signed by *AdvertChain*'s Contract creator private key.

FR-14 The NFT metadata must contain the NFT's name and description, URI of the screenshot, job title, hiring company name, job location, hash of the job description, the original LinkedIn URL, the user's Polygon / Ethereum address, the user's DID, the user's verification VC receipt, the signature and the metadata hash.

FR-15 A REST API endpoint must be created that allows users to verify the authenticity of a LinkedIn job post and the identity of the job poster.

FR-16 A job post must be considered authentic if there is a corresponding NFT for the job post's LinkedIn URL, the NFT's metadata signature matches the job post's details (title, company, location, and description) as retrieved from LinkedIn.

FR-17 A job poster's identity is verified if a) the user DID from the NFT metadata matches the user DID persisted by *AdvertChain* and b) the VC receipt JWT can be verified by the Identity Overlay Network (ION) using the user's DID.

FR-18 The NFT minter must display instructions and FAQ on how *AdvertChain* works.

The system has two main actors: (i) the job poster, who is an employee of the hiring company, authorized to create new job posts and *AdvertChain* NFTs and (ii) the job applicant, who wishes to verify the authenticity of a job post before he/she applies. Following are the main user stories of the *AdvertChain* PoC solution:

1. As a hiring company I want to authorize only my Hiring Managers and Recruiters to create job posts and mint *AdvertChain* NFTs.
2. As a job poster I want to login via LinkedIn, so that I am authenticated.
3. As a job poster I want to validate my identity via my VC, so that I am authorized.
4. As a job poster I want to connect my MetaMask wallet, so that I can mint NFTs.
5. As a job poster I want to be able to mint a LinkedIn job post as NFT, so that I can prove the ownership of the job post to job applicants.
6. As a job applicant I want to verify a job post, so that I know its ownership and identity are authentic before I apply.

The main two methods of this solution are the *mintNFT* method and the *validateJobPost* method. The complexity of the algorithms of both these methods is *O(1)*. The *mintNFT* method of the NFT minter web app is the main method that mints new NFTs for the given LinkedIn job post URLs. The algorithm of this method can be seen in pseudocode in Algorithm 1.

Algorithm 1 Algorithm for minting new *AdvertChain* NFTs

```
1: procedure MINTNFT(url, isAuthenticated, hasValidIdentity)
   ▷ //Validate LinkedIn Identity Federation and Verifiable Credential
2:     if not isAuthenticated || hasValidIdentity then
3:         return 0                                          ▷ //Fail
```

```
    end if
    userLinkedInDetails ← getUserLinkedInDetails()
    userVCclaimDetails ← getVerifiableCredentialDetails()
▷ //Ensure VC claims match the LinkedIn profile
    if userLinkedInDetails != userVCclaimDetails then
        return 0                                                    ▷ //Fail
    end if
▷ //Ensure user's role allows job posting
    if not claimDetails.jobRole in ['Recruiter','HiringManager'] then
        return 0                                                    ▷ //Fail
    end if
▷ //Ensure user works for the same hiring company
    jobPostDetails ← getJobDetailsFromLinkedinPost(url)
    if jobPostDetails.companyName! = userVCclaimDetails.companyName then
        return 0                                                    ▷ //Fail
    end if
▷ //Ensure there are no duplicate NFTs
    jobId ← jobPostDetails.jobId
    userAddr ← getUserEthereumAddrress()
    if nftWithJobIdExists(userAddr, jobId) then
        return 0                                                    ▷ //Fail
    end if
▷ //Create and sign the job post metadata
    screenshot ← getJobPostScreenshot(url)
    metadata ← createMetadata(jobPostDetails, userVCclaimDetails, screenshot)
    signature ← signMetadata(metadata)
    pinScreenshotToIPFS(screenshot)
    tokenURI ← pinMetadataJsonToIPFS(metadata, signature)
▷ //Mint the new NFT and set the owner to the user address
    advertChainContract.methods.mintNFT(userAddr, tokenURI, jobId, signature)
▷ //Store in the DB the userAddr/userDID mapping
    writeToDatabase(userAddr, userVCclaimDetails.DID)
```

The *validateJobPost* serverless function is the main method that validates the authenticity and ownership of a given LinkedIn job post URLs. The algorithm of this method can be seen in pseudocode in Algorithm 2.

Algorithm 2 Algorithm for validating a job post via *AdvertChain*

```
procedure validateJobPost(url)
    jobPostDetails ← getJobDetailsFromLinkedinPost(url)
    jobId ← jobPostDetails.jobId
    metadata ← getMetadataFromIPFS(jobId)
    if metadata == null then
        return 0   ▷ //Ownership cannot be verified. NFT does not exist for the job post
    end if
    userAddr ← metadata.userAddr
    ownerAddr ← advertChainContract.methods.ownerOfJobId(jobId)
    if ownerAddr! = userAddr then
        return 0                                    ▷ //NFT ownership verification failed
    end if
    dbUserDID ← getUserDidFromDatabase(userAddr)
    calculatedMetadata ← createMetadata(jobPostDetails, dbUserDID)
    signature ← signMetadata(calculatedMetadata)
```

```
    if signature! = metadata.signature then
        return 0                          ▷ //NFT metadata and LinkedIn post do not match
    end if
    if dbUserDID! = metadata.userDID then
        return 0                          ▷ //NFT metadata and persisted identity do not match
    end if
▷ //Ensure that the VC receipt JWT was signed by the private key of the user's DID
    didDocument ← ION.RESOLVE(dbUserDID)
    identityVerified ← ION.VERIFYJWS(metadata.vcReceiptJwt,didDocument.publicKeyJwk)
    return identityVerified
```

The *AdvertChain* PoC solution comprises of the following main components:

1. the Web3-enabled NFT minter web application
2. the backend Cloud components (serverless functions and database)
3. the NFT Smart Contract deployed on Polygon on top of the Ethereum Blockchain
4. the integration with Pinata to pin the NFT metadata on IPFS
5. the user identity federation with LinkedIn
6. the Azure Active Directory Verifiable Credentials service
7. the Identity Overlay Network (ION) that stores the DID metadata [2]
8. the W3C Decentralized Identifiers (DIDs) and VCs
9. the DID Wallet (Microsoft Authenticator App)
10. the Verifiable Credentials verifier for the NFT minter
11. a website and a LinkedIn profile for the fake company
12. the Verifiable Credentials issuer for the fake company

Following is the high-level architecture diagram of the *AdvertChain* PoC solution. The main architectural goal of this solution is to be as decentralized as possible. Although a NoSQL database was used in the PoC, when productised the solution will not need to depend on one. Note that the fake company (Dunder Mifflin website, LinkedIn profile, VC issuer and HR system) is not part of the system but it is an external actor and a dependency of the solution. As it can be seen from the diagram, users interact with *AdvertChain* via the frontend and the business logic is delivered via the backend serverless functions. Users mainly interact with *AdvertChain* using a web browser and use the DID/VC wallet (Authenticator app) on their mobile phone to hold and present their Verifiable Credentials to *AdvertChain*. The backend serverless functions handle the VC verification, the identity federation with LinkedIn, the creation of the job post metadata, the creation of the job post screenshot, the pinning of the metadata and the screenshot to IPFS and the minting of the NFTs. To issue and verify proof of employment Verifiable Credentials, the solution uses the Azure AD Verifiable Credentials Service that depends on the Azure Key Vault to store the private keys used for signing the issued VCs.

Figure 3 shows the main actors, components and sequence of steps in a sample use case scenario of issuing and verifying Verifiable Credentials that are used as digital,

[2] https://github.com/decentralized-identity/ion

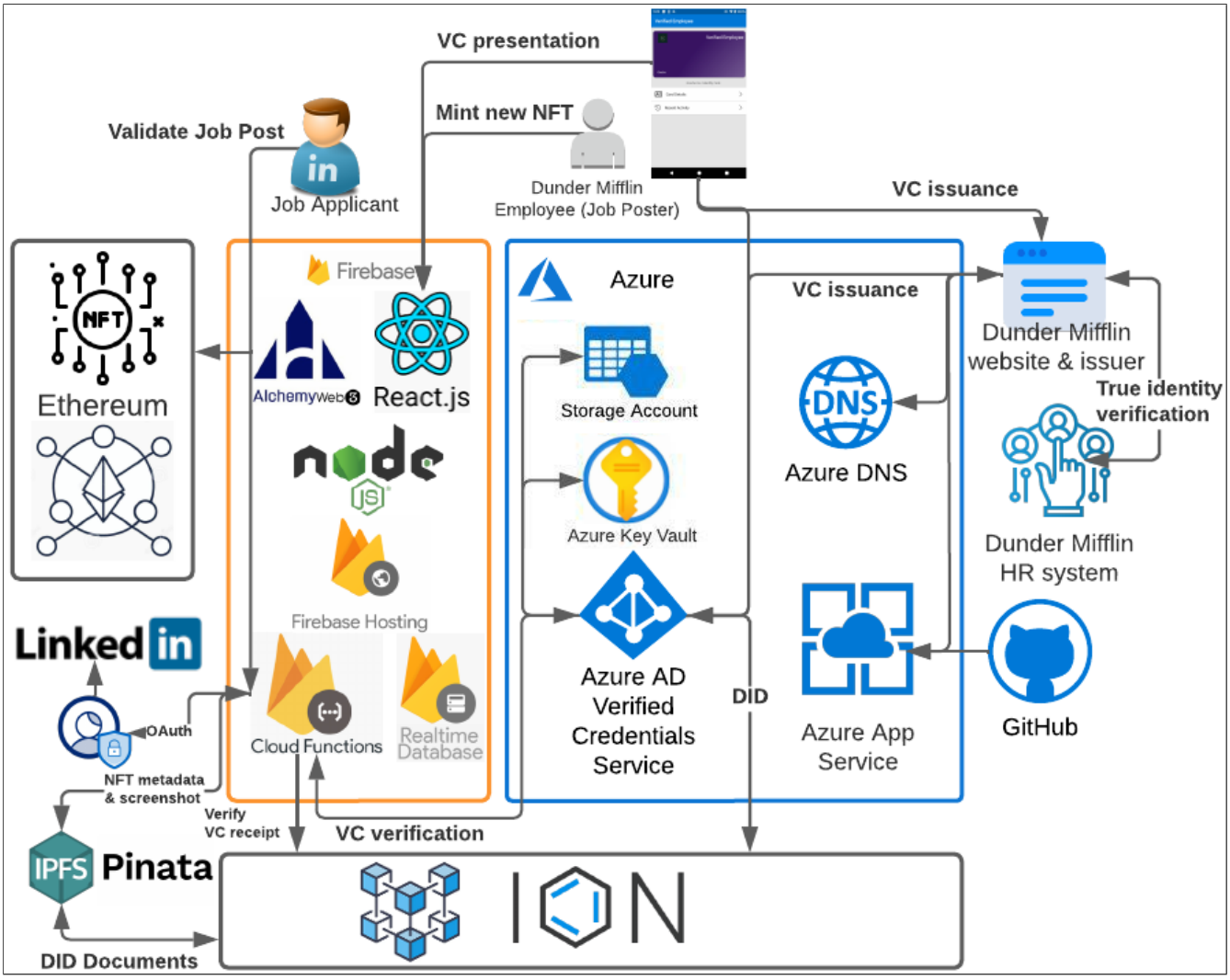

Figure 2: High-level architecture of *AdvertChain*

cryptographically-signed, employment proofs. In the scenario, Michael Scott is a hiring manager at Dunder Mifflin, a fictitious company. Dunder Mifflin has deployed a Verifiable Credential (VC) solution to provide a more manageable way for their employees to prove that they work for Dunder Mifflin. Michael logs into Dunder Mifflin's corporate environment and requests a proof of employment VC using his Authenticator app. Michael scans the QR code generated by Dunder Mifflin. Then, Dunder Mifflin attests Michael's identity and issues a VC with Michael's DID as the subject. The VC is then signed with the company's DID. The newly issued VC is sent back to Michael and it is stored along with its private key in Michael's Authenticator app that acts as a digital wallet. When Michael decides to present this VC as a proof of employment to *AdvertChain*, he visits the *AdvertChain* NFT minter web app where he is presented with another QR code. Michael scans the QR code with his Authenticator app. A few seconds later he is asked to accept the sharing of the VC to *AdvertChain*. Once he accepts, Michael's Authenticator app signs the Verifiable Presentation (VP) with his own DID and sends it to *AdvertChain* for verification. *AdvertChain* then resolves the issuer's DID using the ION network, retrieves its public key and validates authenticity of the VP by verifying its signature using the resolved public key of Dunder Mifflin. After a successful verification, *AdvertChain* authorizes Michael to mint NFTs on behalf of Dunder Mifflin. The VC presentation transaction is logged in Michael's digital wallet application. This way

Michael has total control and visibility regarding where and to whom has has presented his VC. Michael is free to use the same proof of employment VC in many other use cases. During this scenario, Michael's private data are controlled by his Authenticator app. *AdvertChain* receives Michael's private data, uses them only to authorize the user and never persists them in any way. Note that the VC issued by Michael's employer is not bound to *AdvertChain* and can be reused with other verifiers.

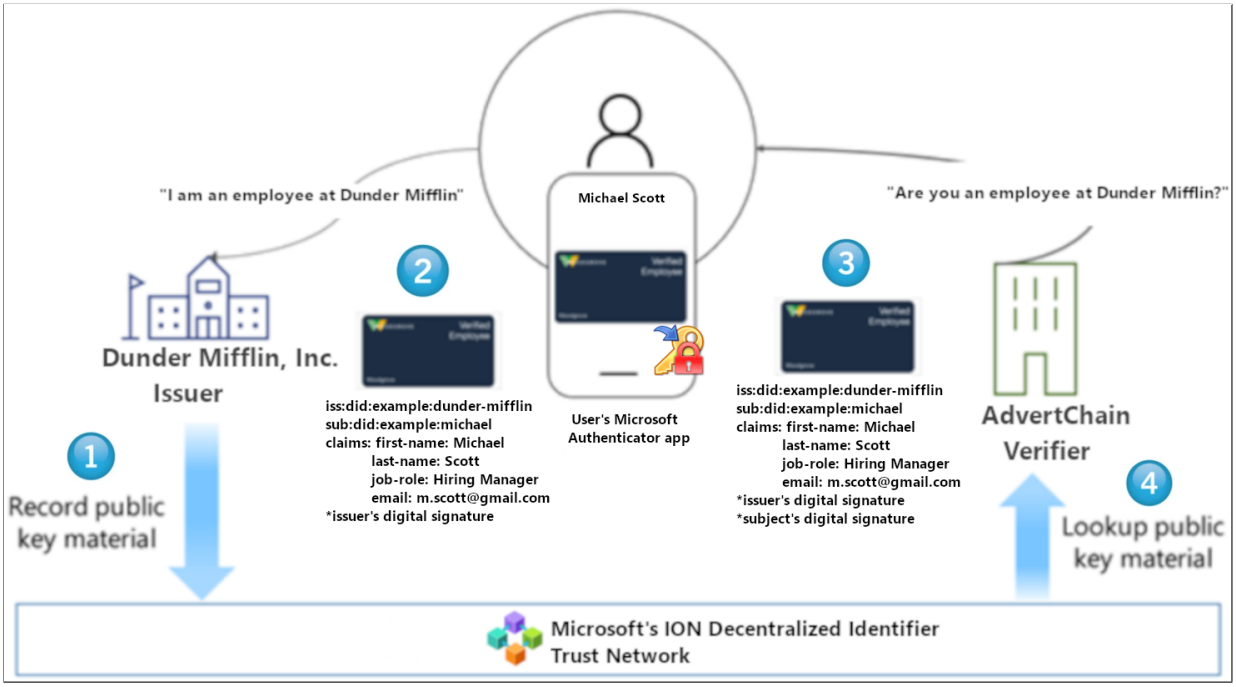

Figure 3: High-level sample use case scenario for VC issuance and verification

5 Implementation

For the implementation of the *AdvertChain* Proof-of-Concept a mixture of technologies, platforms and languages were used. The frontend of the NFT minter web app was implemented using React.js whereas the backend was implemented using Node.js. The integration and interaction with the NFT Smart Contract was done using the Alchemy extension of the Web3 client. The NFT Smart Contract was implemented using Solidity and it was based on the ERC-721 contract of the open-source OpenZeppelin library, which offers standard, tested, and community-reviewed code for building secure Smart Contracts. The prototyping of the NFT Smart Contract and its manual testing was achieved the use of the Remix IDE, whereas the final version was compiled and deployed on Mumbai using Hardhat. Hardhat has also been configured with the *hardhat-etherscan* plugin and an Polygonscan API key that allows the source code of the NFT contract to be published and verified on Polygonscan in order to provide transparency for users interacting with the *AdvertChain* Smart Contract.

Figure 4 shows the source code of the mint method of the *AdvertChain* NFT. Lines 34 and 37 make sure that only the Smart Contract creator can mint new NFTs and sign the metadata. Lines 43 to 48 mint a new NFT with a new token id and assign the ownership to the job poster's Polygon / Ethereum address. The functional requirement FR-7 does not allow the *AdvertChain* NFT to change ownership after it is minted. This is achieved by overriding the internal *_beforeTokenTransfer* method.

To programmatically retrieve a screenshot of the LinkedIn post, a REST API call to the NoCodeAPI platform is sent. To pin the JSON metadata and the screenshot to IPFS, the Pinata SDK was used. Both the frontend and the backend code was deployed on Google's Firebase PaaS platform. The React.js code is hosted on Firebase Hosting service and the Node.js backend code was implemented as serverless Firebase Cloud Functions. The Firebase Realtime Database is used to persist the user's Ethereum addresses and the user's public DID. The *AdvertChain* NFT minter is accessible via https://advertchain-demo.web.app/ and the job post validator is accessible via the REST API endpoint https://us-central1-advertchain-firebase.cloudfunctions.net/api/validateJobPost that accepts the URL of the LinkedIn job post via the *jobUrl* GET query parameter.

To achieve Identity Federation, a developer app for *AdvertChain* was registered on LinkedIn. Using the client ID and the client secret provded by LinkedIn and the configured OAuth 2.0 redirect URL, REST calls with the *r_liteprofile* and *r_emailaddress* were sent from the backend serverless functions to retrieve the federated user's full name and email. To use the Azure AD Verifiable Credentials service, first an Azure Key Vault instance was created in the AAD user tenant. The Azure Key Vault is required by the Verifiable Credentials service to store the public and private keys used to sign, update, and recover VCs. Also, to set up the AAD Verifiable Credentials service, a verified domain name is needed. For this reason, a fake company was created called *Grecho*. Grecho's domain, *www.grecho.site*, was registered via GoDaddy and then was linked to the website hosted on Azure App Service via a new DNS zone that was created on Azure DNS. To verify the domain *www.grecho.site*, a JSON file was deployed that contains the linked DID of the issuer. This is accessible via https://www.grecho.site/.well-known/did-configuration.json. Once the domain was verified, the setup of the VC service completed by registering a new Azure app. Then, the issuing and verification VC service was configured by creating the necessary display and rules JSON files. Finally, a VC issuer for the Grecho domain was created using Node.js, deployed on Azure App Service and it is accessible via https://grecho-vc-issuer.azurewebsites.net. For *AdvertChain* to verify the VC receipt, the open-source ION tools were used that enable interaction with the ION network [3]. Finally, the code that was written for *AdvertChain* and for the *Grecho* website is hosted on two separate Github repositories with enabled GitHub Actions that automate the continuous integration, build and deployment. For the development of the code, the Microsoft Visual Studio Code was used with the Azure extensions configured.

To create the REST API endpoints, the Express web application framework was used and the Express-Session to maintain server-side, in-memory, session store, required for caching VC issuance requests to facilitate QR code scanning. To make REST calls to LinkedIn and to the NoCodeAPI, the Axios HTTP client was used. Finally, to extract the job post data from the LinkedIn job post, the Cheerio library was used.

In terms of coding, the frontend consists of three React components: (i) the NFT minter, which is essentially the main page, (ii) the Profile Card, which contains the user's profile details (full name, email, job role), and (iii) the Social User, which handles the popup window responsible for the LinkedIn Identity Federation. The frontend also consists of the following four React Modal components: (i) the Verifier modal that is responsible for the Verifiable Credential verification, (ii) the FAQ modal that is responsible of displaying a list of frequently asked questions, (iii) the Instructions modal that provides information to the user how to authenticate and get authorization to mint new NFTs, and (iv) the How-It-Works modal that displays some high-level information on

[3] https://github.com/decentralized-identity/ion-tools

how *AdvertChain* works. The main logic for minting new NFTs and for creating the NFT metadata is implemented in the *interact.js* source code file. On the backend, the serverless functions are implemented in the *index.js* file. Finally, the file *callback.js* handles the LinkedIn OAuth callback and returns the authenticated user profile. To avoid leaking secrets, the app uses .env files to load the app's secrets via environmental variables. One of the most important secrets that need to be protected is the private key of the Polygon / Ethereum wallet of the *AdvertChain* NFT creator. A potential leakage of this private key would compromise the security of this solution.

One optimization that was done is the avoidance of creation of duplicate NFT metadata. Due to the fact that the NFT metadata is created and pinned to IPFS before the minting of the NFT, there is a chance of creating duplicate metadata and screenshots on IPFS. To avoid this scenario, the *AdvertChain* NFT minter first verifies if there are pinned metadata or if an NFT has already been minted for the given job id.

Regarding the end-to-end testing of the solution, Postman was used to manually test the REST API endpoints and the Firebase Cloud Function logs were used for debugging. The NFT was tested via the Remix IDE and Polygonscan to manually invoke the Smart Contract's methods. Also, OpenSea was used to verify the *AdvertChain* NFT collection.

```
28 function mintNFT(address recipient, string memory tokenURI, string memory jobId,
29 bytes memory signature, bytes32 hashedMetadata)
30     public
31     returns (uint256)
32 {
33     // make sure that only the contract creator can mint NFTs
34     require(msg.sender == _minter);
35
36     // make sure that the signature has been signed by the contract creator
37     require(recoverSigner(hashedMetadata, signature) == _minter);
38
39     // make sure that we have not minted an NFT for the same job id
40     require(!jobIdExists(jobId),
41             string.concat("ACT: token already minted for the job id: ", jobId));
42
43     _tokenIds.increment();
44
45     uint256 newItemId = _tokenIds.current();
46     _mint(recipient, newItemId);
47     _setTokenURI(newItemId, tokenURI);
48     _jobIds[jobId] = recipient;
49
50     return newItemId;
51 }
```

Figure 4: Source code snippet of the *AdvertChain* NFT mint method

5.1 User Journeys

The main user journey for minting NFTs consists of four very simple steps:

1. User authenticates via LinkedIn. By using Identity Federation via LinkedIn, the authentication process is seamless to the user.

2. User gets authorized by verifying his/her true identity via his/her Verifiable Credential. Users only have to scan the QR code that is presented to them using the Microsoft Authenticator app.
3. Connect the user's MetaMask wallet by clicking the corresponding button.
4. User pastes a link to a LinkedIn job post that was posted by the hiring company the user/job poster works for. Finally, the user presses the "Mint NFT" button.

The main four steps for minting NFTs in *AdvertChain* can be seen in figure 5 that shows a screenshot of the NFT minter app. Note that steps 1-3 are done only once for each user session and step 4 is performed once for every job post that is to be minted as NFT.

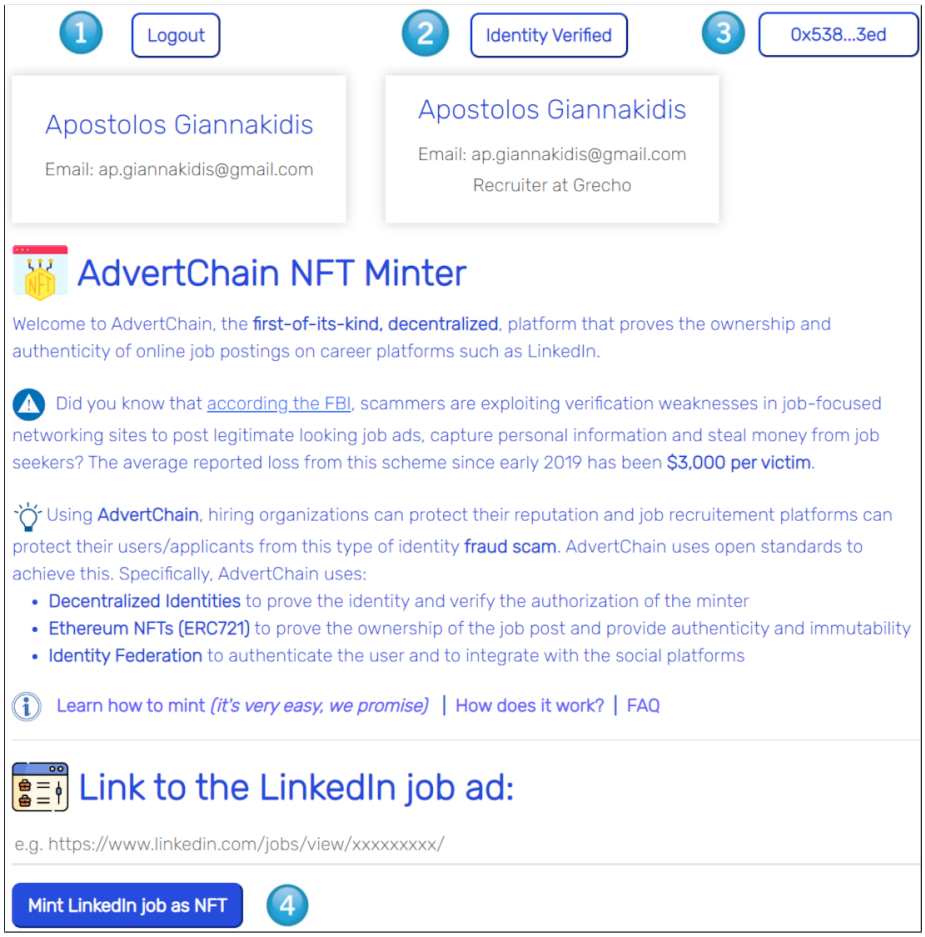

Figure 5: Screenshot of the *AdvertChain* NFT minter portal

The user journey for validating a LinkedIn job post is even simpler, assuming that the user has installed the *AdvertChain* Tampermonkey userscript. The user only needs to visit the job post on LinkedIn. If the ownership of the job post and the identity of the job poster can be validated by *AdvertChain* then a green check is automatically displayed in the job post on LinkedIn, without any further user actions. The job applicant is not required to own a VC, neither to authenticate to *AdvertChain* nor have a digital wallet such as MetaMask installed. Figure 6 shows a screenshot of a successfully validated LinkedIn job post. The green check that was dynamically added by the Tampermonkey userscript can be seen, after proving the job post's validity via *AdvertChain*.

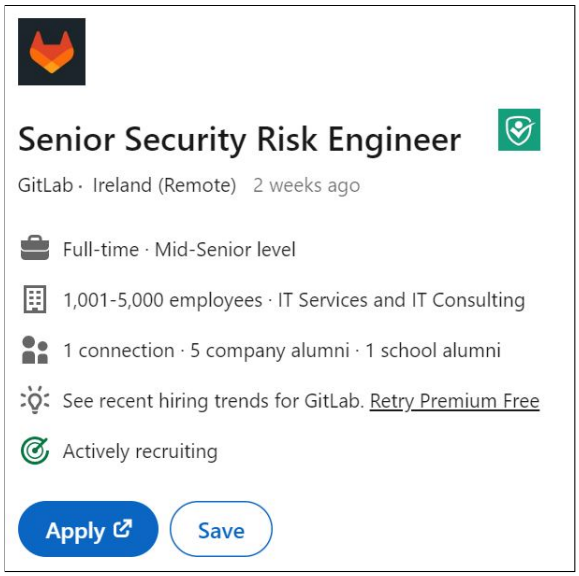

Figure 6: Screenshot of a successfully validated LinkedIn job post by *AdvertChain*

6 Evaluation

6.1 Verification Accuracy

Unlike ML-based solutions, this system does not use any heuristic or probabilistic algorithms. The system validates the ownership of a job post based on the presence of a valid NFT on the Blockchain. Thus, the verification is 100% deterministic. Since *AdvertChain* is still a Proof-of-Concept, only a sample of LinkedIn job posts have been minted. For the ones that have been minted as NFTs, the system verifies their authenticity with 100% accuracy (zero false positives). For the job posts that have not been minted as NFTs the system cannot validate their authenticity. Therefore, if a user tries to validate a fraudulent job post or a legitimate job post that has not been minted as NFT, *AdvertChain* will not report it as authentic and verified. *AdvertChain* becomes most valuable to users who wish to validate the legitimacy of job posts posted by companies that have adopted *AdvertChain* and have minted their job posts as *AdvertChain* NFTs. Thus, the success of this solution depends on the extent of its adoption by the hiring companies.

6.2 Privacy

AdvertChain validates public data and does not store, own, or has access to any user credentials or any other private or sensitive data. Thus, even if the *AdvertChain* backend gets compromised, the malicious users would not have access to any sensitive data. Similarly, there are no personally identifiable information (PII) in the DID Document or its metadata that is stored in the public ION trust network that runs atop of Blockchain. No piece of information in the DID Document can identify a user's identity. The PII is stored encrypted in the Verifiable Credentials on the users' mobile phones.

The privacy of the user who is authorized to mint *AdvertChain* NFTs is preserved because the verification of credentials uses a *Zero-Knowledge-Proof-style* mechanism that does not disclose the identity of the verifiable credential holder to any third party. Also, when job applicants verify the ownership and validity of a job post, they have no access to the identity of the individual who posted the job post or minted the NFT [27].

No private information is stored in the NFT metadata either. The key/value pairs

of the associated metadata store publicly available information (such as information included in the job post) and the *AdvertChain* signature. Finally, in case of privacy or security incidents or other business reasons, issuers may choose to revoke specific Verifiable Credentials. Microsoft's Verifiable Credentials Azure service supports the W3C status property, which permits VCs to be revoked [4].

6.3 Security

One of the security concerns of this solution is the risk of user impersonation in case the mobile device is lost or stolen. Impersonation is not possible due to the fact that the Verifiable Credentials are stored in Microsoft's Authenticator mobile app. The Authenticator app requires users to prove themselves with their fingerprint, face ID, or PIN to access the Verifiable Credentials. Also, by enabling Multi-Factor Authentication (MFA), users make unauthorized access to the app almost impossible.

Regarding the security of the *AdvertChain* ERC-721 smart contract, the risk of a compromise is very small because the mint function contains checks that ensure that (i) only contract creator's address can mint NFTs, (ii) the NFT metadata have been signed by contract creator, and (iii) no duplicate NFTs can be minted for the same job post.

Only the *AdvertChain* frontend has access to the private key of the owner of the Smart Contract. Thus, the system provides the reassurance that no unauthorized user is able to mint NFTs. Additionally, the usage of the NFTs make it impossible for anyone to tamper with the minted data, as it is impossible to change or remove data from the Blockchain. Moreover, because the identity data are not stored on centralized servers, mass data leaks of personal data is not feasible. Also, the strong cryptographic characteristics of the VCs makes them tamper-evident and more trustworthy than their physical counterparts [5].

By relying on Blockchain, the system inherits non-repudiation, authenticity, transparency, and security over every transaction because every transaction is timestamped and digitally signed by each user's wallet.

Finally, the risk of identity theft and Sybil attacks against the reputation of the system is minimised due to the fact that the solution (i) uses biometric access to the VCs on the Authenticator app (ii) utilizes Microsoft's MFA protection layer (iii) gives uses full control of their identity via Decentralized Identifiers (DIDs), (iv) performs authorization checks that ensure that the claims of the verified VC correspond to the federated identity and (v) the NFTs can only be signed and minted by the Smart Contract owner.

6.4 User Experience

For the success of a software solution, one important factor is the simplicity of its use and its ability to provide a meaningful experience to its users. For this reason, the User Interface has been designed with simplicity in mind, so that even the most basic users would be able to follow the steps.

The fact that *AdvertChain* users do not have to sign-up and create new accounts makes the user experience seem effortless. This is because users save time and effort from going through the sign-up process as well as because they do not have to remember new usernames and passwords.

The user verification process requires only three simple and straightforward steps, while the NFT minting process only requires copy pasting the URL of the job post and clicking a button. Both of these processes typically take less than one minute to complete.

[4] https://docs.microsoft.com/en-us/azure/active-directory/verifiable-credentials/how-to-issuer-revoke

The job post verification is even easier to follow. Essentially, assuming that users have installed the *AdvertChain* Tampermonkey userscript, they only need to visit the job post of interest on LinkedIn. The Tampermoneky userscript automatically displays the green check icon if the job's ownership and posters identity can be verified. No user action is needed. For more advanced users or a third-party developers, the provided REST API endpoint can be used for programmatic access. The API endpoint only accepts a single parameter; the job post URL that needs to be verified.

Thus, it can be seen from the above that the *AdvertChain* solution is very easy to use even by the most basic users. This simplicity in its usage could be an important factor in achieving adoption by the community.

6.5 Extensibility

One of the advantages of using Identity Federation is that *AdvertChain* can integrate with more job-related social platforms, apart from LinkedIn. In fact, if *AdvertChain* gets productised and gets released in a General Availability version, then it will be necessary to establish trust with more social Identity Providers (IdPs) and allow users to mint online job posts from multiple job-related social platforms. This will be achieved with a seamless user experience as it will not affect how the user authentication process.

Also, since *AdvertChain* only depends on the link to the job post, providing support to mint online job posts from multiple job-related social platforms will be very straightforward in terms of application development.

6.6 Cost Analysis

The design choice of using NFTs and Blockchain comes with a cost. Minting NFTs requires the minter to pay a transaction fee. *AdvertChain* currently uses the Polygon network, which uses *MATIC* tokens for the transaction fees. *AdvertChain* does not assign a value to its NFTs and neither mints the NFTs on marketplaces. This means that the only cost for minting NFTs is the Polygon gas fee, which lowers the operational costs.

The *AdvertChain* Proof-of-Concept uses Mumbai, which is a Polygon testnet. Using the testnet, there is no real cost for minting NFTs. Thus, for testing purposes, using *AdvertChain* is free as there are no minting costs. However, if *AdvertChain* gets productised, there will be real costs for minting NFTs due to the Polygon transaction fees. Polygon supports *lazy-minting*, which is a way to mint NFTs completely free, however *lazy-minting* is not applicable in our scenario because *AdvertChain* NFTs are never traded.

Minting NFTs on Polygon mainnet has significantly lower and more predictable transaction fees compared to Ethereum. According to the Polygon Gas Tracker [4], at the time of writing, the gas fee on Polygon was around 60 to 80 *Gwei*. *Gwei* are fractions of Ether (ETH), which is the native token of the Ethereum Blockchain. The Ethereum gas fees depend on the amount of data used but also on the speed of the transaction, the time of day due to demand on the network and the current price of the USD/Ether pair [28]. As an indication, the Ethereum transaction fees could range between US$50 on average but might reach over US$100 during periods of high volume of traffic. On the Polygon network, minting an NFT could incur transaction fees as low as $0.01.

Thus, using Polygon for this solution is a cost-effective choice. Being cost-effective is a critical factor for the adoption of *AdvertChain*, considering that many hiring companies will be minting tens of NFTs per month.

[4] https://polygonscan.com/gastracker/

6.7 Performance

To evaluate the performance and scalability of the system, the response time of the *validateJobPost* serverless function was measured for different numbers of minted NFTs. The average response times were measured by sending via JMeter 1k requests after minting 10, 20, 40, 60, 80 and 100 NFTs. As it can be seen from the data of the diagram at Figure 7, it is safe to assume that the system's validation performance does not get negatively impacted by the total number of minted NFTs. This is achieved due to the decentralized design of the system as well as the efficient algorithms, as described in the design section. Additionally, the Google/Firebase Cloud Functions scale automatically the number of compute instances based on the number of incoming requests. Thus, the system has the ability to scale up automatically depending on the the load.

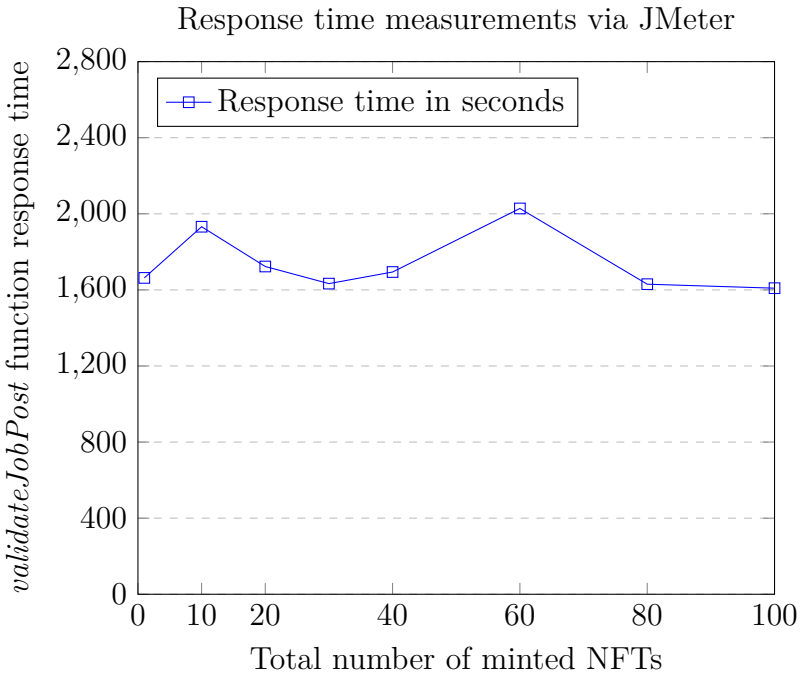

Figure 7: Job post validation response time dependence on the number of minted NFTs

6.8 Discussion

The main goal of this research is to provide a protection mechanism against the online job post scam. This solution aims to protect the job applicants, however, unlike the ML-based solutions in the literature review, this proposed solution requires the active participation of the hiring companies and the job posters. By validating the ownership of the job post and the identity of the job poster, this solution manages to overcome the language limitation, that is one of the limiting factors of the ML-based solutions. Additionally, this solution's verification model is deterministic with zero false positives, unlike the heuristic verification model of the ML-based solutions. By taking advantage of the unique, decentralized, properties of NFTs and DIDs, this solution creates trust between the job recruitment platforms, the hiring companies, the job posters and the job applicants. It also provides data integrity and it increases security, privacy, transparency, and traceability.

7 Conclusion and Future Work

This research project introduced a prototype decentralized solution that aims to address the identity-theft that exploits the job posting scam from popular career-networking platforms, as described by the FBI's recent public service announcement (I-020122-PSA). The prototype solution, *AdvertChain*, leverages public Cloud services, Blockchain, Decentralized Identifiers, public key cryptography and Identity Federation to provide ownership and identity verification to online job posts. After the users have been authenticated and authorized, they mint LinkedIn job posts as NFTs on the Blockchain. Representing job posts as NFTs allows *AdvertChain* to provide unique digital certificate of ownership for each job post. Additionally, associating each minted NFT with the DID of each verified user, *AdvertChain* can provide secure and true user identity verification.

By exploring the literature review on the job posting scam, evidence was provided for the novelty and the feasibility of the proposed solution. This report provided a detailed design specification and a comprehensive description of the PoC implementation. Finally, an evaluation of the solution was given that includes an extensive analysis of the most important aspects of the solution such as its accuracy, security and privacy. By evaluating the proposed solution, it can be determined that *AdvertChain* achieves its main goal of securely verifying job posts with deterministic accuracy, achieving 100% accuracy for the job posts that have been minted as NFTs, while preserving the user's privacy.

This solution's main challenge is its adoption by the major career-networking platforms and the hiring companies. If *AdvertChain* gets adopted by the major career-networking platforms, the overall success rate of the job posting scam will be reduced significantly, resulting in the saving of tens of thousands of US dollars every year.

In the future, the solution would benefit by adding support for the following features:

1. Integrate with more career platforms, such as Indeed and Glassdoor. This will increase the solution's interoperability and impact and it will be a critical factor in establishing *AdvertChain* as the de-facto solution against the job posting scam.
2. Implement the Sign-In-with-Ethereum (SIWE) standard (EIP-4361). Using Web3 authentication signatures, the backend will be able to securely verify the client-side user's wallet address.
3. Perform authorization of the users on the server-side instead on the client-side. Currently, this is done on the client-side for rapid development of the Proof-of-Concept. However, the authorization checks must be performed on the server side in the future, to avoid malicious users from minting NFTs for job posts that they are unauthorized. This is currently possible because the logic of the client-side authorization checks can be manipulated maliciously.
4. Add a personalised view that displays to the authenticated users the NFTs that each user has minted. Currently, this is possible via NFT marketplaces such as Opensea, however Opensea is meant to be used for trading NFTs, which is not applicable to the *AdvertChain* NFTs.
5. Blockchains with cheaper transaction fees should be explored. Assess if using the Amazon Managed Blockchain would be a cheaper solution operationally.
6. *AdvertChain* has been designed to address the online job scam, however, the same concept could be used to protect other digital assets. *AdvertChain* could be extended to add support to other types of digital assets with minimal code modifications.

References

[1] Shareen Irshad and Tariq Rahim Soomro. Identity theft and social media. *International Journal of Computer Science and Network Security*, 18(1):43–55, 2018.

[2] Gavin Wood. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, 2014.

[3] Wei Cai, Zehua Wang, Jason B. Ernst, Zhen Hong, Chen Feng, and Victor C. M. Leung. Decentralized applications: The blockchain-empowered software system. *IEEE Access*, 6:53019–53033, 2018. doi: 10.1109/ACCESS.2018.2870644.

[4] Nitin Naik and Paul Jenkins. Self-sovereign identity specifications: Govern your identity through your digital wallet using blockchain technology. In *2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)*, pages 90–95, 2020. doi: 10.1109/MobileCloud48802.2020.00021.

[5] Manu Sporny, Dave Longley, and David Chadwick. Verifiable credentials data model. *World Wide Web Consortium (W3C)*, March 2022. Available at https://www.w3.org/TR/vc-data-model/, version 1.1.

[6] Andrew Hughes, Manu Sporny, and Drummond Reed. A primer for decentralized identifiers. *World Wide Web Consortium (W3C)*, November 2022. Available at https://w3c-ccg.github.io/did-primer/.

[7] Clemens Brunner, Ulrich Gallersdörfer, Fabian Knirsch, Dominik Engel, and Florian Matthes. Did and vc:untangling decentralized identifiers and verifiable credentials for the web of trust. In *2020 the 3rd International Conference on Blockchain Technology and Applications*, ICBTA 2020, page 61–66, New York, NY, USA, 2020. Association for Computing Machinery. ISBN 9781450388962. doi: 10.1145/3446983.3446992.

[8] D. Rountree. *Federated Identity Primer*. Elsevier Science, 2012. ISBN 9780124072077.

[9] Sokratis Vidros, Constantinos Kolias, and Georgios Kambourakis. Online recruitment services: another playground for fraudsters. *Computer Fraud Security*, 2016 (3):8–13, 2016. ISSN 1361-3723. doi: https://doi.org/10.1016/S1361-3723(16)30025-2.

[10] Sokratis Vidros, Constantinos Kolias, Georgios Kambourakis, and Leman Akoglu. Automatic detection of online recruitment frauds: Characteristics, methods, and a public dataset. *Future Internet*, 9(1):6, 2017.

[11] Syed Mahbub and Eric Pardede. Using contextual features for online recruitment fraud detection. In *Designing Digitalization*, 2018. ISBN 978-91-7753-876-9.

[12] Okti Nindyati and I Gusti Bagus Baskara Nugraha. Detecting scam in online job vacancy using behavioral features extraction. In *2019 International Conference on ICT for Smart Society (ICISS)*, volume 7, pages 1–4. IEEE, 2019.

[13] Sultana Umme Habiba, Md. Khairul Islam, and Farzana Tasnim. A comparative study on fake job post prediction using different data mining techniques. In *2nd International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST)*, pages 543–546, 2021. doi: 10.1109/ICREST51555.2021.9331230.

[14] Bodduru Keerthana, Anumala Reethika Reddy, and Avantika Tiwari. Accurate prediction of fake job offers using machine learning. In Debnath Bhattacharyya and N. Thirupathi Rao, editors, *Machine Intelligence and Soft Computing*, pages 101–112, Singapore, 2021. Springer Singapore. ISBN 978-981-15-9516-5.

[15] C.S. Anita, P. Nagarajan, G. Sairam, P. Ganesh, and G. Deepakkumar. Fake job detection and analysis using machine learning and deep learning algorithms. *Revista Gestão Inovação e Tecnologias*, 11:642–650, 06 2021. doi: 10.47059/revistageintec.v11i2.1701.

[16] Paula Fraga-Lamas and Tiago M. Fernández-Caramés. Fake news, disinformation, and deepfakes: Leveraging distributed ledger technologies and blockchain to combat digital deception and counterfeit reality. *IT Professional*, 22(2):53–59, 2020. doi: 10.1109/MITP.2020.2977589.

[17] Adnan Qayyum, Junaid Qadir, Muhammad Umar Janjua, and Falak Sher. Using blockchain to rein in the new post-truth world and check the spread of fake news. *IT Professional*, 21(4):16–24, 2019. doi: 10.1109/MITP.2019.2910503.

[18] Qian Chen, Gautam Srivastava, Reza M. Parizi, Moayad Aloqaily, and Ismaeel Al Ridhawi. An incentive-aware blockchain-based solution for internet of fake media things. *Information Processing Management*, 57(6):102370, 2020. ISSN 0306-4573. doi: https://doi.org/10.1016/j.ipm.2020.102370.

[19] P. Freni, E. Ferro, and G. Ceci. Fixing social media with the blockchain. In *Proceedings of the 6th EAI International Conference on Smart Objects and Technologies for Social Good*, GoodTechs '20, page 175–180, New York, NY, USA, 2020. Association for Computing Machinery. ISBN 9781450375597. doi: 10.1145/3411170.3411246.

[20] Wee Jing Tee and Raja Kumar Murugesan. Trust network, blockchain and evolution in social media to build trust and prevent fake news. In *2018 Fourth International Conference on Advances in Computing, Communication Automation (ICACCA)*, pages 1–6, 2018. doi: 10.1109/ICACCAF.2018.8776822.

[21] Amna Qureshi and David Megías Jiménez. Blockchain-based multimedia content protection: Review and open challenges. *Applied Sciences*, 11, 2021. ISSN 2076-3417. doi: 10.3390/app11010001.

[22] Tao Jiang, Aina Sui, Weiguo Lin, and Pengbin Han. Research on the application of blockchain in copyright protection. *2020 International Conference on Culture-oriented Science Technology (ICCST), Culture-oriented Science Technology (ICCST), 2020 International Conference on, ICCST*, pages 616 – 621, 2020. ISSN 978-1-7281-8138-7.

[23] Ma Zhaofeng, Huang Weihua, and Gao Hongmin. A new blockchain-based trusted drm scheme for built-in content protection. *EURASIP Journal on Image and Video Processing*, 2018:1–12, 2018.

[24] Sijia Zhao and Donal O'Mahony. Bmcprotector: A blockchain and smart contract based application for music copyright protection. ICBTA 2018, page 1–5, New York, NY, USA, 2018. Association for Computing Machinery. ISBN 9781450366465. doi: 10.1145/3301403.3301404.

[25] Dongjie Liu, Wei Wang, Yang Wang, and Yaling Tan. Phishledger: A decentralized phishing data sharing mechanism. In *Proceedings of the 2019 International Electronics Communication Conference*, IECC '19, page 84–89, New York, NY, USA, 2019. Association for Computing Machinery. ISBN 9781450371773. doi: 10.1145/3343147.3343154.

[26] Laura Pirro. How agile project management can work for your research. *Nature*, 04 2019. doi: 10.1038/d41586-019-01184-9.

[27] Galia Kondova and Jörn Erbguth. Self-sovereign identity on public blockchains and the gdpr. In *Proceedings of the 35th Annual ACM Symposium on Applied Computing*, pages 342–345, 2020.

[28] Giuseppe Antonio Pierro and Henrique Rocha. The influence factors on ethereum transaction fees. In *2019 IEEE/ACM 2nd International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB)*, pages 24–31, 2019. doi: 10.1109/WETSEB.2019.00010.