

Elevating Android Privacy: A Blockchain-Powered Paradigm for Secure Data Management

Bang Khanh Le^{*1}, Ngan Thi Kim Nguyen², Khiem Gia Huynh³, Phuc Trong Nguyen⁴,
Anh The Nguyen⁵, Khoa Dand Tran⁶, Trung Hoang Tuan Phan^{*7}
FPT University, Can Tho City, Viet Nam^{1,3,4,5,6,7}
FPT Polytechnic, Can Tho City, Viet Nam²

Abstract—The significance of medical test records in diagnosing and treating illnesses cannot be overstated. These records serve as the foundation upon which medical professionals craft precise treatment strategies tailored to a patient’s unique health condition and ailment. However, in several developing nations, such as Vietnam, a concerning trend persists: medical test records predominantly exist in vulnerable paper format, entrusted to patients for safekeeping. When patients transition between healthcare facilities, the responsibility of carrying these paper-based medical histories rests with them, introducing a significant risk factor due to the inherent fragility of paper documents, which can be easily damaged by fire or water. The loss of these crucial records can lead to severe disruptions in the diagnostic and therapeutic journey of patients, potentially compromising their well-being. Despite the emergence of various alternatives to address this vulnerability, Vietnam faces multifaceted challenges. These challenges encompass low technological literacy among patients and substantial infrastructural limitations. In response to these pressing issues, this study endeavors to harness the transformative potential of blockchain technology, smart contracts, and Non-Fungible Tokens (NFTs) to effectively mitigate the drawbacks associated with paper-based medical test records. Our comprehensive approach includes meticulous cataloging of current hospital practices, the introduction of a purpose-built blueprint for decentralized record sharing, the proposal of an innovative NFT-backed authentication model, the development of a practical proof-of-concept, and comprehensive platform testing. Through these efforts, we aim to revolutionize the management of medical test records in Vietnam, enhancing accessibility, security, and reliability for both patients and healthcare providers.

Keywords—Medical test result; blockchain; smart contract; NFT; Ethereum; Fantom; Polygon; Binance smart chain

I. INTRODUCTION

The ubiquity of Android applications (apps) in contemporary society is undeniable. These apps have seamlessly woven themselves into the fabric of daily life, offering indispensable utility across various domains. Whether it’s navigation through Google Maps, social connectivity via Facebook, or health tracking with Fitbit, Android apps have become indispensable companions to billions of users. As of March 2023, the Google Play store boasts an astounding repository of over 2.6 million apps¹, a testament to the Android ecosystem’s enduring popularity and expansion. The significance of Android’s prevalence extends beyond mere numbers. According to App Annie’s 2021 report, Android users collectively spent an astonishing 3.5 trillion hours on these apps². This level of

engagement underscores the integral role Android apps play in modern life. To exemplify, consider Facebook, one of the most pervasive Android apps, with an impressive 2.94 billion monthly active users. Remarkably, 1.96 billion users visit the social networking platform daily³. Yet, in tandem with this digital revolution comes a growing concern about privacy. A 2019 Pew Research Center report revealed that approximately 81% of the public feels they have little or no control over the data collected about them, be it by private companies or government entities⁴. This concern extends to mobile apps, as demonstrated by a 2019 survey by NortonLifeLock, which found that 72% of consumers worry about their privacy when using these apps. Concerns range from the specter of identity theft to fears of unauthorized access to personal information⁵. In response to these privacy concerns, Android introduced a permission model for managing access to sensitive data and specific actions within apps⁶. This model empowers users by requiring apps to request permissions, which can be granted or denied during installation or at runtime. App stores like the Google Play Store implement review processes and policies to ensure app compliance with privacy guidelines. This enables users to review app permissions, ratings, and user feedback, equipping them with the tools to make informed decisions regarding privacy risks⁷. Additionally, data safety policies mandate developers to be transparent about their data practices, ensuring data protection⁸.

However, traditional methods for safeguarding user privacy within Android apps face significant challenges. Centralized data storage, a prevalent feature in these apps, introduces a “single point of failure” that substantially heightens the risk of data breaches and unauthorized access [1]. Moreover, these traditional methods often lack transparency, rendering it difficult for users to comprehend and control how their data is collected, processed, and shared. This lack of transparency can erode user trust and deter them from using a service due to privacy concerns [2], [3]. Additionally, these methods offer limited user control over personal data, constraining users from managing what data is collected, how it’s used, or with whom it’s shared [4]. Recognizing the urgency of addressing these challenges, this paper introduces a novel and forward-thinking approach to elevate Android app privacy to new

³<https://bit.ly/3CzGfbo>

⁴pewrsr.ch/3PjVOLW

⁵<https://bit.ly/447dheI>

⁶<https://developer.android.com/guide/topics/permissions/overview?hl=en>

⁷For instance, TikTok’s privacy policy can be found at: <https://www.tiktok.com/legal/page/row/privacy-policy/en>

⁸<https://bit.ly/467Mkct>

¹<http://bit.ly/3Nduhcg>

²<https://technologymagazine.com/digital-transformation/app-annie-38-trillion-hours-spent-mobiles-2021>

heights. Our contribution centers on a groundbreaking hybrid architecture that integrates conventional data processing with blockchain technology, tailored specifically to handle sensitive data. The importance of this contribution cannot be overstated. As the Android app ecosystem continues to expand, so do the volumes of data being generated and processed, including sensitive health and medical data. With the growing emphasis on user privacy, our hybrid approach offers a transformative paradigm that ensures advanced security, transparency, and user control. It provides a solution to the persistent privacy concerns pervasive within the Android app ecosystem.

In this paper, we delve into the intricacies of our hybrid architecture, demonstrating how it effectively manages 'dangerous' permissions, particularly those related to motion/health/medical data, which are of paramount importance due to their sensitivity. Through rigorous evaluation on Ethereum Virtual Machine (EVM) compatible platforms such as BNB, Fantom, Celo, and Matic, we identify the optimal platform, with the Fantom platform emerging as a standout choice owing to its low transaction costs and optimal gas limits. Additionally, our paper outlines comprehensive strategies for persuading service providers and Android OS producers to adopt our transformative approach. By doing so, we present a pioneering perspective on the application of blockchain technology to address the persistent privacy concerns that continue to challenge the Android app ecosystem. In the subsequent sections, we provide a detailed account of our approach, the evaluation results, and the strategies for adoption, ultimately contributing to a future where Android users can enjoy the benefits of innovative apps without compromising their privacy.

II. RELATED WORK

In this section, we provide an extensive review of related work in the field of privacy preservation within Android platforms. While our paper introduces a novel approach leveraging blockchain technology for this purpose, it is essential to contextualize our contribution within the broader landscape of existing research.

A. Malware Analysis

Privacy preservation within Android platforms has long been a concern, prompting researchers to explore various methodologies to address these challenges. One prominent avenue of research in this area is malware analysis, which focuses on identifying and mitigating malicious software that may compromise user privacy.

Talha et al. [5] developed APK Auditor, a system designed for detecting malicious apps through permission analysis. This multifaceted system encompassed Android clients, a signature database, and a central server. APK Auditor employed static analysis to capture permission requests and calculate malicious scores, contributing to the early efforts of enhancing Android app security.

In a similar vein, Jianmao et al. [6] introduced MPDroid, an innovative approach that evaluated the risk of target apps based on minimum permissions. The methodology incorporated collaborative filtering and clustering techniques to assess app risk,

providing valuable insights into permission-based privacy risk estimation.

Enck et al. [7] proposed TaintDroid, an Android platform extension that significantly advanced privacy preservation. This pioneering system tracked the flow of privacy-sensitive data within third-party apps and promptly labeled apps as privacy violations when personal data was transmitted to third parties. TaintDroid marked a critical milestone in privacy-aware app development and user protection.

Furthermore, Moutaz et al. [8] focused on a set of dangerous permissions identified by Google⁹, contributing to the categorization and understanding of potential privacy risks within Android apps.

While these studies made commendable strides in enhancing privacy preservation within Android platforms, they often provided binary detection outcomes (malicious or benign). This binary nature of their analysis might not be sufficient to assist users effectively in their decision-making processes.

To address this limitation, Son et al. [4], [9] proposed an innovative approach centered on risk estimation based on an app's data collection and sharing behavior. Their approach marked a significant shift towards a more nuanced understanding of app privacy risks, enabling users to make informed choices based on the level of risk they were willing to accept. Additionally, their app recommendation system [10] further personalized user app choices based on their privacy preferences, contributing to user-centric privacy preservation.

However, even these advanced risk estimation approaches do not fully address the need for a robust, transparent, and user-controlled platform for managing sensitive data within Android apps. In contrast, our paper introduces a novel paradigm by integrating blockchain technology into Android platforms. This blockchain-based system offers enhanced security, transparency, and user control for handling sensitive data, thereby providing a balanced, secure, and effective method for managing data in Android apps. By retaining traditional processing for 'normal' data, our approach preserves app functionality and data processing effectiveness. Our contribution represents a significant advancement in the ongoing efforts to protect user privacy on Android platforms.

B. Sensitive Data Encryption

Another prevalent approach to privacy preservation within Android platforms is sensitive data encryption. This methodology involves encoding user data in a way that allows only authorized parties to access it, thus ensuring the confidentiality and integrity of sensitive information.

Chen et al. [11] proposed AUSERA, an automated tool designed to detect security vulnerabilities in Android apps. While AUSERA did not specifically focus on encryption, its contribution lay in the identification of security vulnerabilities, which are often associated with privacy breaches.

Zhang et al. [12] examined the vulnerability of Android external storage, an area susceptible to data leakage, and proposed solutions to prevent sensitive information disclosure.

⁹<https://developer.android.com/reference/android/Manifest.permission>

Their work underscored the importance of protecting sensitive data, especially in scenarios where external storage is involved.

Fan et al. [13] introduced HPDROID, an automated system that identified GDPR compliance violations in mobile health applications. While their primary focus was on compliance, it indirectly contributed to privacy preservation by highlighting the critical need for robust data protection mechanisms within health-related apps.

Mia et al. [14] conducted a comprehensive comparative study on HIPAA technical safeguards assessment of Android mHealth applications. This study provided valuable insights into healthcare data privacy, emphasizing the need for stringent security measures within healthcare apps.

Hauptert et al. [15] evaluated the state of Android app hardening and identified vulnerabilities in a leading Runtime Application Self-Protection (RASP) product. Their work demonstrated the need for continuous improvement in security mechanisms to protect sensitive data from emerging threats.

Chen et al. [16] and Sengupta et al. [3] proposed blockchain-based systems specifically designed for preserving medical data privacy within Android platforms. These pioneering contributions recognized the unique challenges associated with healthcare data and demonstrated the potential of blockchain technology in safeguarding sensitive medical information.

Balasubramaniam et al. [17] conducted a comprehensive survey on data privacy and preservation using blockchain in healthcare organizations. This survey illuminated emerging trends and challenges in healthcare data privacy, underscoring the importance of innovative solutions like blockchain.

While these studies have made valuable contributions to privacy preservation within Android platforms, they often rely on developers' security knowledge and diligence. Moreover, some studies focus primarily on healthcare data and do not address the broader range of sensitive data handled by Android apps. Others lack a specific implementation tailored for Android platforms.

In contrast, our proposed blockchain-based system offers a robust, transparent, and user-controlled platform for managing sensitive data in Android apps, applicable to a wide array of data types beyond healthcare. By integrating blockchain technology, we address the limitations of existing approaches and contribute significantly to the ongoing endeavor to preserve user privacy on Android platforms.

III. BACKGROUND

A. Android OS and Permission System

Android, an open-source operating system developed by Google, is ubiquitous in modern society, powering a wide array of mobile devices such as smartphones, tablets, and wearables. Built upon the Linux kernel, Android offers a robust application framework, enabling developers to create innovative apps and games within a Java-based environment. This extensive ecosystem boasts over 2.6 million apps available on the Google Play Store as of March 2023, highlighting its profound impact on our digital lives. Central to Android's design is its intricate permission system, meticulously crafted

to safeguard user privacy. This system plays a pivotal role in dictating how apps interact with sensitive user data and device resources. When developers create an Android app, they must explicitly define in the app's manifest file what types of permissions the app requires to function effectively. These permissions govern a diverse range of access, from location data to contacts, camera, microphone, and beyond.

Permissions in the Android ecosystem are categorized into different levels, with particular emphasis on two primary types: Normal and Dangerous permissions. The distinction between these permission categories is crucial and forms the cornerstone of user privacy and security:

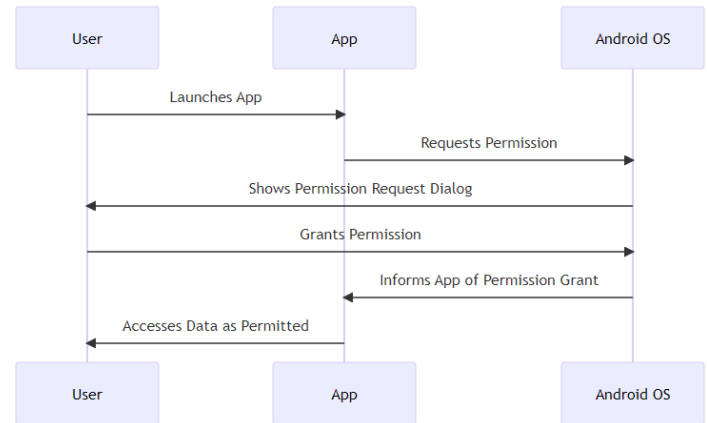


Fig. 1. The user data collection via the permission system in android OS.

- **Normal Permissions:** These permissions encompass scenarios where apps need to access data or resources outside their own sandboxed environment, with minimal risk to user privacy or the functioning of other apps. An example of a normal permission is the ability to set the device's time zone. Such permissions are typically granted without explicit user consent at installation.
- **Dangerous Permissions:** In contrast, dangerous permissions involve access to highly sensitive user data or device resources, potentially affecting user privacy and the integrity of other apps. Permissions like accessing the user's contacts, camera, or location fall into this category. Android mandates explicit user consent for granting dangerous permissions, often soliciting consent dynamically as the app requires access during runtime, rather than at installation.

The Android permission system operates as a crucial pillar in maintaining a balance between app functionality and user privacy. It empowers users to make informed decisions regarding which permissions to grant to individual apps, ensuring their data remains secure and their privacy respected.

Fig. 1 illustrates the intricate workflow involved in an app's data collection via the Android permission system. This process embodies the essence of user-centric privacy preservation within the Android ecosystem.

In summary, Android's widespread adoption and sophisticated permission system have fostered an environment where

user data privacy is paramount. However, challenges remain in ensuring transparent, secure, and user-controlled data management, especially concerning sensitive information.

B. Blockchain Technology

Blockchain technology has emerged as a disruptive force, initially popularized through its association with digital currencies like Bitcoin. Its inherent properties have extended far beyond the realm of cryptocurrencies, finding applications across diverse industries. At its core, a blockchain consists of a chain of blocks, each containing a list of transactions. These blocks are cryptographically linked, with each new block referencing the previous one, creating an immutable ledger. Immutability ensures that once data is recorded on the blockchain, it cannot be retroactively altered, providing unparalleled data integrity. One of the foundational characteristics of blockchain technology is its decentralization. Unlike traditional centralized databases, where a single entity controls access and data, a blockchain operates on a network of distributed nodes. Each node holds a complete copy of the blockchain and participates in validating and recording new transactions. This decentralized architecture eliminates single points of failure and dramatically enhances security. Transparency and auditability are fundamental attributes of blockchain technology. All transactions on the blockchain are visible to every participant in the network. Moreover, every transaction is permanently recorded, creating an unchangeable audit trail. This transparency builds trust and accountability, assuring participants that no transaction can be tampered with or erased.

Smart contracts, another hallmark feature of blockchain, are self-executing agreements with contract terms directly encoded into code. These contracts automatically execute transactions when predefined conditions are met, removing the need for intermediaries. In the context of Android privacy preservation, blockchain technology offers a range of benefits:

- **Enhanced Data Security:** Blockchain replaces centralized data storage with a decentralized, tamper-resistant mechanism. Advanced cryptographic algorithms and distributed consensus protocols secure user data against unauthorized access, manipulation, or breaches. This significantly mitigates the risk associated with centralized data storage and bolsters privacy preservation in Android systems.
- **Improved Transparency and Auditing:** Traditional methods for managing user data in Android apps often suffer from a lack of transparency, causing trust issues among users. Blockchain's transparency and immutability address this problem. Every transaction is transparent and can be audited, ensuring app developers and service providers adhere to declared privacy policies and data handling practices. Smart contracts provide an auditable trail of all data interactions, increasing transparency and fostering user trust.
- **User Control and Consent:** One significant drawback of conventional methods is the limited control users have over their personal data. Blockchain technology significantly enhances user control over personal data. With self-sovereign identity solutions built on

blockchain, users can manage their own identity data, decide what information to share, and with whom, and for what purpose. These features offer users the ability to selectively consent to data collection and sharing, substantially preserving their privacy.

- **Data Integrity and Provenance:** The immutable nature of blockchain ensures the integrity and provenance of data. Each data transaction is recorded permanently and cannot be altered, providing a verifiable and auditable history of data transactions. This feature allows users to verify the authenticity and accuracy of their data, enhancing the trustworthiness of Android apps, particularly in scenarios where data traceability and accountability are paramount.
- **Secure Data Sharing:** Blockchain technology can also facilitate secure and controlled data sharing within the Android ecosystem. Users can grant or revoke access to their data at any time with blockchain-based consent management systems. This flexibility ensures that data is only shared with authorized parties and only for approved purposes, further enhancing privacy preservation in Android applications.
- **Trust and Collaboration:** The distributed and transparent nature of blockchain technology inherently fosters trust and collaboration among participants. By providing a shared and immutable record of data transactions, blockchain can help establish trust between users, app developers, and service providers in the Android ecosystem. This enhanced trust can encourage responsible data handling practices, promote fair data exchanges, and motivate collaborative efforts in privacy preservation, leading to a more secure and user-centric Android platform.

In summary, the intersection of Android OS and blockchain technology holds great promise for addressing the challenges associated with privacy preservation in the Android app ecosystem. The combination of Android's extensive user base and the robust security and transparency offered by blockchain creates a compelling framework for reimagining how sensitive data is managed and protected in mobile applications.

IV. APPROACH

Our proposed approach, depicted in Fig. 2, represents a comprehensive integration of blockchain technology with the permission management process in Android systems. This integration is meticulously designed to bolster privacy preservation and provide users with heightened control over their sensitive data.

To elucidate the intricacies of our approach, we break it down into a series of steps, each serving a crucial role in ensuring robust privacy protection and user empowerment:

Step 1: User Application Installation The journey begins when a user decides to install an application, with a particular focus on medical applications. Medical apps are chosen for their inherent sensitivity, as even small fragments of medical data hold the potential for privacy breaches, potentially compromising individual identities.

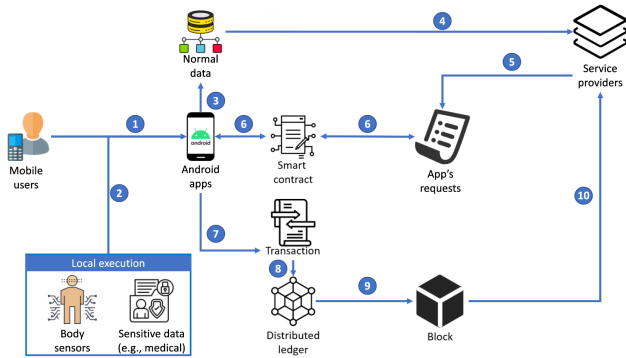


Fig. 2. Architecture of our proposed privacy-preserving model.

Step 2: Dangerous Permission Request When a medical application requests access to sensitive medical data through Android's dangerous permissions system, it potentially gains access to the user's comprehensive or aggregated health information. This marks the second step in our process.

Step 3: Normal Data Request In cases where the application requests access to non-sensitive, normal data, it follows the conventional permissions procedure outlined in Section III. Such data can be collected without the need for additional security measures.

Step 4: Secure Data Transmission Should the service provider necessitate the transmission of the collected normal data to their servers (referred to as "global execution"), the fourth step of our approach comes into play. Our system ensures the secure and encrypted transmission of this data to the designated service provider's servers.

Step 5: Sensitive Data Request Alternatively, if an application seeks sensitive data, such as those accessed via dangerous permissions like `BODY_SENSORS` and `BODY_SENSORS_BACKGROUND` for medical data collection, it is mandated to provide detailed information regarding the purpose of usage, the specific data types required, and the possibility of third-party involvement. This meticulous process is justified by (i) the availability of most of this information in the application's privacy policy and (ii) compliance with data privacy regulations, including the General Data Protection Regulation (GDPR)¹⁰, which mandates secure data handling processes by applications.

Step 6: User Validation via Smart Contract The user, on their mobile device, actively participates in the decision-making process concerning their data in the sixth step. This active involvement is facilitated through the use of smart contracts, which enhance transparency and decentralize control, placing it squarely in the hands of the user.

Step 7: Transaction Logging Upon user validation, the decision is meticulously logged as a transaction, creating a formal agreement between the user and the service providers. This transactional logging process harkens back to the conventional permission system. However, it takes a significant leap forward by incorporating machine learning techniques, which enable future decisions to reference these initial agreements. This reduces the need for recurrent user interventions [18].

Step 8: Secure Storage in Distributed Ledger All these transactions, replete with user decisions and service provider agreements, are securely stored within a distributed ledger (DLT) in the eighth step. This distributed ledger serves as an immutable repository of records, rendering every transaction traceable and tamper-resistant.

Step 9: Encryption and Non-Fungible Tokens (NFTs) The ninth step involves the encryption of user responses using the service provider's public key, employing elliptic curve cryptography [19]. This ensures that only the intended service provider can decrypt and access the user's responses. To further bolster data security and uniqueness, we utilize Non-Fungible Token (NFT) technology to encapsulate these responses. Each NFT is designed to be distinct and non-interchangeable, safeguarding the integrity and confidentiality of user data.

Step 10: Data Transfer via NFTs The final step in our approach is the seamless transfer of these NFT-encapsulated user responses to the service provider. This culminating interaction furnishes the service provider with the requisite and authorized data, while concurrently creating a traceable, indelible record of the transaction on the blockchain.

Our architectural approach presents numerous advantages over the traditional Android permission system:

- **Enhanced Transparency and Auditability:** The integration of blockchain technology ensures that every transaction is meticulously recorded and verifiable, offering a heightened level of transparency and auditability.
- **User Empowerment and Control:** The use of smart contracts places the reins of control firmly in the hands of the user. Users can distinctly specify which data can be accessed, fostering greater empowerment and autonomy.
- **Data Integrity and Secure Sharing:** By leveraging NFTs and elliptic curve cryptography, our approach guarantees data integrity and secure data sharing. This ensures that sensitive data remains confidential and unaltered.
- **Trust Building and Regulatory Compliance:** Our innovative approach facilitates trust-building between users and service providers. Furthermore, it promotes collaborative data sharing while adhering to stringent data privacy regulations.
- **Scalability and Efficiency:** The inherent scalability and efficiency of blockchain technology position our approach as a sustainable choice for future privacy-preserving systems, capable of meeting evolving demands and challenges.

In conclusion, our comprehensive integration of blockchain technology with the Android permission process represents a significant leap forward in privacy preservation and user-centric control over sensitive data. By embedding transparency, security, and efficiency into the core of our approach, we aim to redefine data privacy in the digital age.

V. EXPERIMENTS

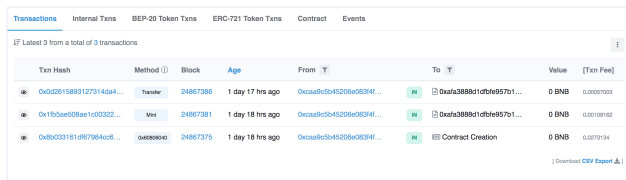
Our research endeavors to introduce a blockchain-based platform that operates as a distributed ledger, with a primary

¹⁰<https://gdpr-info.eu/>

focus on the intricacies of steps 8 and 9, as illustrated in Fig. 2. This phase marks a pivotal step toward our overarching research objective.

A. Methodology

In the development of our platform, we meticulously considered various blockchain platforms that offer support for the Ethereum Virtual Machine (EVM). The selected platforms, including Binance Smart Chain (BNB Smart Chain)¹¹; Polygon¹²; Fantom¹³; and Celo¹⁴, were chosen over open-source alternatives such as those within the Hyperledger ecosystem (e.g., Hyperledger Fabric) due to their compatibility with EVM and their widespread adoption within the decentralized application (DApp) development community. As a critical facet of our research, we implemented our approach across four distinct blockchain platforms that support the Ethereum Virtual Machine (EVM): BNB Smart Chain (BNB), Polygon (MATIC), Fantom (FTM), and Celo (CELO). An essential contribution of this study is the comprehensive collection and analysis of transaction fees associated with these platforms, utilizing their respective testnet coins. All implementations have been made publicly accessible, underscoring our commitment to contributing to the broader blockchain community. Within our evaluation, we paid meticulous attention to transaction fees and gas limits, both of which have profound implications for the operational costs and efficiency of deploying DApps on blockchain networks. Transaction fees represent the costs associated with processing a transaction and fluctuate depending on factors such as transaction complexity and network congestion. Gas limits, on the other hand, dictate the maximum amount of computational resources (gas) a user is willing to expend on a transaction, safeguarding against inadvertent overspending.



Transaction Hash	Method	Block	Age	From	To	Value	[Txn Fee]
0x0420158831273145a4...	Transfer	24867385	1 day 17 hrs ago	0x0a95b945206e083f4f...	0x0a3888810b9495701...	0 BNB	0.0007003
0x1f0aee00bae1c03022...	Mint	24867381	1 day 18 hrs ago	0x0a95b945206e083f4f...	0x0a3888810b9495701...	0 BNB	0.00109162
0x06033161d87984cc6...	Contract Creation	24867375	1 day 18 hrs ago	0x0a95b945206e083f4f...	0 BNB	0.00057003	

Fig. 3. Transaction information (e.g., BNB Smart Chain).

Our evaluation involved the assessment of three fundamental functions on each of these platforms:

- 1) ****Creating User Responses:**** This pivotal function embodies the user's consent level, signifying their stance on data collection, whether it involves denying data access, permitting partial access, or granting full access to medical data, as expounded in Section IV.
- 2) ****Creating Non-Fungible Tokens (NFTs):**** The user's response is encrypted using the service provider's public key and subsequently encapsulated into an NFT. This process ensures both the integrity and confidentiality of user responses.

¹¹ <https://github.com/bnb-chain/whitepaper/blob/master/WHITEPAPER.md>

¹² <https://polygon.technology/lightpaper-polygon.pdf>

¹³ <https://whitepaper.io/document/438/fantom-whitepaper>

¹⁴ <https://celo.org/papers/whitepaper>

- 3) ****Transferring NFTs:**** Subsequently, the NFT is transferred to the service provider, solidifying an immutable record of the user's response.

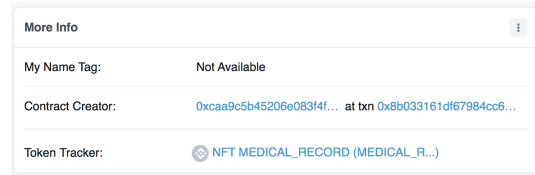


Fig. 4. NFT creation

While encryption plays a pivotal role in our approach, we have intentionally refrained from delving into the intricacies of encryption methodologies within this paper due to the substantial scope involved. A more exhaustive exploration of encryption methodologies and their analysis will be presented in forthcoming iterations of this research. Fig. 3 offers a glimpse into one of our evaluations, specifically detailing a successful deployment on the BNB Smart Chain. Analogous procedures and assessments were meticulously carried out across the remaining three platforms. Smart contracts, developed using the Solidity programming language, constituted the core of our evaluations. We scrutinized the execution costs of these contracts within the testnet environments of the respective platforms, with a primary objective of ascertaining the most cost-efficient platform for deploying our system. We delved into the intricacies of contract creation, NFT generation (as depicted in Fig. 4), and NFT ownership address updates, a process fundamentally revolving around retrieving and transferring NFTs (refer to Fig. 5).

B. Transaction Fee Analysis

In our investigation, we conducted an in-depth analysis of transaction fees incurred during the operations of Contract Creation, NFT Creation, and NFT Transfer across four prominent blockchain platforms: BNB Smart Chain, Fantom, Polygon (MATIC), and Celo. The results of this comparative analysis are summarized in Table I. On the BNB Smart Chain, the transaction fees for Contract Creation, NFT Creation, and NFT Transfer amounted to 0.0273134 BNB (\$8.43), 0.00109162 BNB (\$0.34), and 0.00057003 BNB (\$0.18), respectively. The Fantom platform exhibited lower transaction costs, with Contract Creation priced at 0.00957754 FTM (\$0.001849), NFT Creation at 0.000405167 FTM (\$0.000078), and NFT Transfer at 0.0002380105 FTM (\$0.000046). The Polygon (MATIC) platform showcased even more economical costs, with Contract Creation incurring 0.006840710032835408 MATIC (\$0.01), NFT Creation incurring 0.000289405001852192 MATIC (almost negligible in USD terms), and NFT Transfer incurring 0.000170007501088048 MATIC (also nearly negligible in USD terms). Finally, the Celo platform reported fees of 0.007097844 CELO (\$0.004) for Contract Creation, 0.0002840812 CELO (almost negligible in USD terms) for NFT Creation, and 0.0001554878 CELO (also nearly negligible in USD terms) for NFT Transfer.

This comprehensive analysis highlights the substantial variability in transaction fees across the four platforms, underscor-

TABLE I. TRANSACTION FEES (IN NATIVE TOKENS AND USD EQUIVALENTS)

	Contract Creation	Create NFT	Transfer NFT
BNB Smart Chain	0.0273134 BNB (\$8.43)	0.00109162 BNB (\$0.34)	0.00057003 BNB (\$0.18)
Fantom	0.00957754 FTM (\$0.001849)	0.000405167 FTM (\$0.000078)	0.0002380105 FTM (\$0.000046)
Polygon	0.006840710032835408 MATIC (\$0.01)	0.000289405001852192 MATIC (almost negligible)	0.000170007501088048 MATIC (almost negligible)
Celo	0.007097844 CELO (\$0.004)	0.0002840812 CELO (almost negligible)	0.0001554878 CELO (almost negligible)

ing the critical importance of platform selection in optimizing the cost-effectiveness of deploying our approach.

C. Gas Limit Assessment

TABLE II. GAS LIMITS FOR OPERATIONS

	Contract Creation	Create NFT	Transfer NFT
BNB Smart Chain	2,731,340	109,162	72,003
Fantom	2,736,440	115,762	72,803
Polygon	2,736,284	115,762	72,803
Celo	3,548,922	142,040	85,673

In addition to transaction fees, gas limits represent a vital facet when deploying smart contracts on Ethereum-based platforms. Gas limits delineate the upper bound of computational resources (gas) allocated to a transaction, serving as a safeguard against inadvertent overspending. Table II summarizes the gas limits associated with various operations, including Contract Creation, NFT Creation, and NFT Transfer, across the four blockchain platforms under consideration: BNB Smart Chain, Fantom, Polygon (MATIC), and Celo.

On the BNB Smart Chain, the gas limits for Contract Creation, NFT Creation, and NFT Transfer stand at 2,731,340, 109,162, and 72,003, respectively.

In the Fantom platform, the corresponding gas limits are marginally higher, with Contract Creation at 2,736,440, NFT Creation at 115,762, and NFT Transfer at 72,803.

Polygon (MATIC) records similar gas limits, with Contract Creation at 2,736,284, NFT Creation at 115,762, and NFT Transfer at 72,803.

Lastly, the Celo platform exhibits the highest gas limits among the four platforms. Contract Creation incurs a gas limit of 3,548,922, NFT Creation requires 142,040 gas, and NFT Transfer necessitates 85,673 gas.

This detailed analysis underscores the substantial variations in gas limits across the four platforms, further emphasizing the need for meticulous consideration in selecting the most suitable platform for deploying our innovative approach.

VI. DISCUSSION

The paradigm of secure data management and privacy preservation on Android devices has been a persistent challenge in the digital age. Our proposed approach, which integrates blockchain technology into the Android permission process, represents a transformative shift in how we address this challenge. In this discussion, we delve deep into the implications and significance of our approach, considering its potential to elevate Android privacy to new heights.

A. Blockchain as the Guardian of Privacy

The integration of blockchain technology into Android's data permission management brings about a fundamental transformation. One of the core advantages is the transparency and immutability inherent to blockchain. Every transaction, every access request, and every decision made by users are recorded in an unalterable ledger. This ledger serves as a comprehensive audit trail, granting users unprecedented visibility into how their data is accessed and used. The user-centric transparency aligns with the overarching theme of elevating Android privacy, allowing users to exercise greater control over their sensitive data. Moreover, blockchain introduces the concept of decentralized control. Through smart contracts, users actively participate in granting or denying access to their data. This not only empowers users but also shifts the locus of control from centralized authorities to individual users. The notion of users as stewards of their data is a critical step toward achieving robust data privacy.

B. User-Centric Data Control

Central to our approach is the pivotal role of smart contracts in the decision-making process. Users validate data access requests through these contracts, granting consent or withholding it. This mechanism puts the power back in the hands of users, enabling them to specify precisely which data can be accessed and under what circumstances. This level of fine-grained control is a substantial departure from the traditional Android permission system, which tends to be binary and all-encompassing. Our approach aligns perfectly with the ethos of user-centric data control. Users are no longer passive participants; they are active decision-makers in the data access process. This newfound agency fosters trust between users and service providers, as users have confidence that their data is used according to their wishes. It also complies with emerging data privacy regulations, such as the General Data Protection Regulation (GDPR), which emphasize user consent and control over personal data.

C. Security and Integrity via NFTs and Cryptography

Data security is a paramount concern in Android privacy, especially when dealing with sensitive information like medical data. Our approach addresses this concern through the use of Non-Fungible Tokens (NFTs) and elliptic curve cryptography. NFTs encapsulate user responses in a unique and non-interchangeable manner. This uniqueness guarantees that user responses remain distinct and unforgeable. It bolsters data integrity and confidentiality, assuring users that their data is protected from tampering or unauthorized access. Elliptic curve cryptography further fortifies data security. By encrypting user responses with the service provider's public key, we ensure that only the designated service provider can decrypt and access the data. This cryptographic layer adds an additional barrier to unauthorized data access.

Txn Hash	Age	From	To	Token ID	Token
0x0d2615893127314da4...	1 day 18 hrs ago	0xaf3888d1dfbfe957b1...	OUT 0xcaa9c5b45206e0834f...	1	ERC-721: NFT....ORD
0x1fb5ae508ae1c00322...	1 day 18 hrs ago	0x000000000000000000...	IN 0xaf3888d1dfbfe957b1...	1	ERC-721: NFT....ORD

[\[Download CSV Export\]](#)

Fig. 5. NFT transfer.

D. Trust Building and Regulatory Compliance

The elevation of Android privacy through blockchain-powered data management also contributes to trust-building between users and service providers. Users are more likely to engage with applications and services when they are confident that their data is handled with care and transparency. This trust-building aspect is essential for the sustained growth of the Android ecosystem. Additionally, our approach aligns seamlessly with data privacy regulations like GDPR. Compliance with these regulations is not just a legal requirement but also an ethical obligation. By facilitating user consent, control, and transparency, our approach inherently complies with these stringent privacy regulations. This alignment ensures that service providers can operate with confidence in a regulatory landscape that increasingly prioritizes data privacy.

E. Scalability and Efficiency

The scalability and efficiency of blockchain technology make our approach a viable and sustainable choice for the future. As Android ecosystems evolve and expand, the need for scalable privacy solutions becomes increasingly pronounced. Blockchain's inherent capacity to handle a growing volume of transactions positions our approach as a robust solution for the long term. Moreover, the efficiency of our approach is underscored by the use of various blockchain platforms, such as Binance Smart Chain, Fantom, Polygon (MATIC), and Celo. The comparative analysis of transaction fees and gas limits across these platforms offers insights into cost-effective deployment options. The adaptability of our approach to multiple blockchain environments ensures that it can seamlessly integrate into a diverse range of Android applications and services.

In conclusion, our blockchain-powered paradigm for secure data management on Android devices represents a groundbreaking approach to elevate Android privacy. By introducing transparency, user-centric control, data security, trust-building, and scalability, we lay the foundation for a new era of Android privacy that aligns with evolving user expectations and regulatory requirements.

VII. CONCLUSION

In this paper, we have introduced a groundbreaking approach aimed at enhancing privacy and data security for Android applications, with a specific focus on the sensitive domain of medical apps. Leveraging the capabilities of blockchain technology, our novel approach has been designed to fundamentally transform the way privacy preservation is addressed within Android platforms. Our comprehensive architecture ensures robust controls on permissions, enforces transparency in data transactions, and places users at the forefront

of data management, thereby significantly elevating Android privacy standards. The central premise of our approach is the integration of blockchain technology into the Android ecosystem, revolutionizing how user data is accessed, utilized, and protected. We have presented a detailed architectural framework that harnesses the power of blockchain to regulate access to sensitive user data. This framework extends beyond the conventional Android permission system, offering a multi-step process that heightens the security and transparency of data interactions.

Through our rigorous evaluation on four Ethereum Virtual Machine (EVM)-supported platforms, namely Binance Smart Chain (BNB), Polygon (MATIC), Fantom (FTM), and Celo (CELO), we have demonstrated the feasibility and effectiveness of our approach. Notably, our evaluation revealed that the Fantom platform emerged as the most suitable option for our work. The low transaction costs and optimal gas limit settings make it an attractive choice for implementing our privacy-preserving framework. However, we acknowledge that the cryptocurrency market is subject to fluctuations, and these results may evolve over time. In our discussion, we have recognized that the successful deployment of our approach hinges on the acceptance and adoption by key stakeholders, including service providers and Android OS producers. We have outlined strategies to garner support from these critical actors, underlining the value of our approach in achieving enhanced privacy and data security.

Looking ahead, our future work will delve into the measurement and enhancement of encryption methodologies to further fortify data privacy and mitigate potential risks. As technology continues to advance, our research makes a substantial contribution to the ongoing discourse surrounding user privacy and data security within the Android ecosystem. We firmly believe that our work lays the essential foundation for the development of more transparent, secure, and user-friendly Android applications. By aligning with the evolving expectations of users and complying with ever-stricter data privacy regulations, our approach is poised to lead the way towards a future where Android privacy reaches new heights.

ACKNOWLEDGMENT

Our sincere appreciation is extended to Engineer Le Thanh Tuan and Dr. Ha Xuan Son, whose expertise and guidance have been indispensable in the brainstorming, execution, and assessment phases of this project. Additionally, the continuous support from FPT University Cantho Campus, Vietnam, has been instrumental in the fruition of this work.

REFERENCES

- [1] E. Bandara *et al.*, "A blockchain and self-sovereign identity empowered digital identity platform," in *2021 International Conference on*

- Computer Communications and Networks (ICCCN)*. IEEE, 2021, pp. 1–7.
- [2] S. Al-Natour *et al.*, “An empirical investigation of the antecedents and consequences of privacy uncertainty in the context of mobile apps,” *Information Systems Research*, vol. 31, no. 4, pp. 1037–1063, 2020.
- [3] A. Sengupta *et al.*, “User control of personal mhealth data using a mobile blockchain app: design science perspective,” *JMIR mHealth and uHealth*, vol. 10, no. 1, 2022.
- [4] H. X. Son, B. Carminati, and E. Ferrari, “A risk assessment mechanism for android apps,” in *2021 IEEE International Conference on Smart Internet of Things (SmartIoT)*. IEEE, 2021, pp. 237–244.
- [5] K. A. Talha *et al.*, “Apk auditor: Permission-based android malware detection system,” *Digital Investigation*, vol. 13, pp. 1–14, 2015.
- [6] J. Xiao *et al.*, “An android application risk evaluation framework based on minimum permission set identification,” *Journal of Systems and Software*, vol. 163, p. 110533, 2020.
- [7] W. Enck *et al.*, “Taintdroid: an information-flow tracking system for realtime privacy monitoring on smartphones,” *ACM Transactions on Computer Systems (TOCS)*, vol. 32, no. 2, pp. 1–29, 2014.
- [8] M. Alazab *et al.*, “Intelligent mobile malware detection using permission requests and api calls,” *Future Generation Computer Systems*, vol. 107, pp. 509–521, 2020.
- [9] H. X. Son, B. Carminati, and E. Ferrari, “A risk estimation mechanism for android apps based on hybrid analysis,” *Data Science and Engineering*, vol. 7, no. 3, pp. 242–252, 2022.
- [10] —, “Priapp-install: Learning user privacy preferences on mobile apps’ installation,” in *Information Security Practice and Experience: 17th International Conference*. Springer, 2022, pp. 306–323.
- [11] S. Chen *et al.*, “Ausera: Automated security vulnerability detection for android apps,” in *37th IEEE/ACM International Conference on Automated Software Engineering*, 2022, pp. 1–5.
- [12] H. Zhang *et al.*, “Protecting data in android external data storage,” in *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)*, vol. 1. IEEE, 2019, pp. 924–925.
- [13] M. Fan *et al.*, “An empirical evaluation of gdpr compliance violations in android mhealth apps,” in *2020 IEEE 31st international symposium on software reliability engineering (ISSRE)*. IEEE, 2020, pp. 253–264.
- [14] M. R. Mia *et al.*, “A comparative study on hipaa technical safeguards assessment of android mhealth applications,” *Smart Health*, vol. 26, p. 100349, 2022.
- [15] V. Hauptert *et al.*, “Honey, i shrunk your app security: The state of android app hardening,” in *Detection of Intrusions and Malware, and Vulnerability Assessment: 15th International Conference*. Springer, 2018, pp. 69–91.
- [16] Z. Chen *et al.*, “A blockchain-based preserving and sharing system for medical data privacy,” *Future Generation Computer Systems*, vol. 124, pp. 338–350, 2021.
- [17] S. Balasubramaniam *et al.*, “A survey on data privacy and preservation using blockchain in healthcare organization,” in *International Conference on Advance Computing and Innovative Technologies in Engineering*. IEEE, 2021, pp. 956–962.
- [18] H. X. Son *et al.*, “In2p-med: Toward the individual privacy preferences identity in the medical web apps,” in *International Conference on Web Engineering*. Springer, 2023, pp. 126–140.
- [19] D. Hankerson *et al.*, *Guide to elliptic curve cryptography*. Springer Science & Business Media, 2006.