FORENSIC ANALYSIS OF CRYPTOCURRENCY TRANSACTIONS: INSIGHTS FROM ANDROID DEVICES CONNECTED TO HARDWARE WALLETS

Van Ba Tai[1], Chen Min Huang[2]

[1]*Faculty of Engineering, Dong Nai Technology University, Bien Hoa City, Vietnam*
[2]*College of Intelligent Science & Technology, I-Shou University, Kaohsiung City, Taiwan*
*Corresponding author: *Van Ba Tai, vanbatai@dntu.edu.vn*

GENERAL INFORMATION

Received date: 26/03/2024

Revised date: 03/05/2024

Accepted date: 11/07/2024

KEYWORD

Cryptocurrency forensics;
Android devices;
Hardware wallets;
Artifact analysis;
Blockchain transactions.

ABSTRACT

While blockchain ledgers publicly record cryptocurrency transactions, the anonymity of transaction participants presents challenges for forensic investigation. This study concentrates on analyzing android device-based cryptocurrency transactions tethered to hardware wallets: D'cent Biometric Wallet and Ledger Nano S. Through meticulous scrutiny of artifacts produced by these tools – we engineered CryptoInfoGetter; an application designed to extract data related to cryptocurrencies. We developed the tool 'CryptoInfoGetter' for extracting cryptocurrency-related data from artifacts generated by two specific hardware wallets--the D'cent Biometric Wallet and Ledger Nano S; this development was a result of our analysis into forensic aspects of Android device-connected crypto transactions. Our analysis unveils valuable insights: wallet details; transaction histories and hardware wallet configurations—these provide pivotal evidence for forensic investigations. We also confront challenges--the dynamic nature of transactions, anonymity features in particular—and deliberate over opportunities to bolster investigative techniques. The advancement of cryptocurrency forensic analysis necessitates indispensable collaboration among researchers, law enforcement personnel, as well as industry stakeholders.

1. INTRODUCTION

Cryptocurrencies, epitomized by Bitcoin, have emerged as a disruptive force in the realm of finance, promising decentralized and pseudonymous transactions through the innovative use of blockchain technology (Suratkar et al., 2020). While this technology offers unparalleled transparency in recording transactions on a distributed ledger, it also presents challenges in the realm of forensic investigation, particularly regarding the anonymity of transaction participants. This anonymity feature has unfortunately been exploited by nefarious actors for illicit activities, ranging from money laundering to the facilitation of illegal transactions (Qi et al., 2022; Saeed Rasheed et al., 2023; Uddin et al., 2021).

In the context of combating such illicit activities, forensic analysis plays a pivotal role in unraveling the complexities of cryptocurrency transactions. One of the critical challenges faced by forensic investigators lies in tracing these transactions back to their originators, a task made increasingly difficult when utilizing hardware wallets – secure devices designed to store cryptocurrency keys offline (Aiolli et al., 2019; Thomas et al., 2020). Unlike traditional centralized exchanges, which often require personal verification, hardware wallets offer users a level of anonymity that complicates the process of tracking and attributing transactions (Dmitrienko et al., 2017; M. M. Mirza et al., 2022).

Our research tackles this challenge: we conduct forensic analysis on artifacts that Android devices connected to hardware wallets generate. We specifically delve into examining the database files produced by two leading hardware wallets - D'cent Biometric Wallet and Ledger Nano S- when operated with Android devices; this investigation aims to address a crucial issue—extracting valuable cryptocurrency-related information—with potential application in criminal investigations where misuses of cryptocurrencies are involved (He et al., 2020; Khan et al., 2019; D. Mirza & Rahulamathavan, 2023).

To address these challenges, our study focuses on analyzing artifacts generated by hardware wallet applications used on Android devices. We investigated two specific hardware wallets: the D'cent Biometric Wallet and the Ledger Nano S. Our analysis involved examining the database files created by these applications to uncover critical information such as wallet details, transaction histories, and hardware wallet configurations. We developed a forensic tool named CryptoInfoGetter to facilitate the extraction and analysis of cryptocurrency-related data from these artifacts.

Key findings from our research include the identification of significant data within the default.realm file of the D'cent Wallet and the AsyncStorage file of Ledger Live, which are crucial for tracing cryptocurrency transactions and identifying hardware wallet configurations. Our study demonstrated that the artifacts from these applications can provide valuable evidence for constructing timelines of transactions and understanding wallet usage. Additionally, the research highlights the effectiveness of CryptoInfoGetter in simplifying the extraction process, offering a practical solution for forensic investigators. These findings underscore the potential of artifact analysis in enhancing the capabilities of cryptocurrency forensics and addressing the challenges associated with anonymous digital transactions.

In this paper, we present the findings of our analysis, detailing the methodologies employed, the types of information obtained, and the implications for forensic investigations. Additionally, we introduce CryptoInfoGetter, a tool developed based on our research findings, which facilitates the extraction and analysis of cryptocurrency-related data from Android devices. Through this research, we seek to contribute to the advancement of forensic techniques in combating cryptocurrency-related crimes and to stimulate further inquiry into this burgeoning field.

2. RELATED WORKS

The forensic analysis of cryptocurrency transactions has been a subject of considerable research interest, driven by the widespread adoption of cryptocurrencies and the challenges posed by their pseudonymous nature. Scholars have explored various methodologies for analyzing blockchain transactions to trace the flow of cryptocurrencies and identify illicit activities, leveraging techniques such as blockchain analytics and graph-based analysis. Additionally, there has been a growing focus on the forensic analysis of hardware wallets, which store cryptocurrency keys offline, necessitating the development of techniques for

extracting and analyzing data from these devices to uncover evidence of illicit transactions. Mobile devices, particularly Android smartphones, have also been the subject of forensic analysis, with researchers examining application data and system files to recover cryptocurrency-related artifacts such as wallet addresses and transaction histories. A plethora of tools and techniques have been developed to aid in cryptocurrency forensic investigations, including blockchain explorers, wallet analyzers, and specialized forensic software. Moreover, legal and ethical considerations surrounding cryptocurrency forensic analysis, such as user privacy and data protection, have also been explored to ensure compliance with relevant laws and regulations. By building upon and extending the findings of previous research in these areas, our study aims to contribute to the development of effective forensic techniques for combating cryptocurrency-related crimes and enhancing the security of blockchain ecosystems. The comparison of some current related works with their advantages and disadvantages in relation to the proposed tool, CryptoInfoGetter, shown in Table 1.

Table 1. Comparison of Cryptocurrency Forensic Tools: Advantages and Disadvantages Relative to CryptoInfoGetter

Related Work	Chainalysis Reactor	CipherTrace	FTK Imager	X1 Social Discovery	EnCase Forensic
Advantages	Comprehensive blockchain analysis. - Provides detailed transaction mapping. - Well-established in the industry.	Advanced analytics for cryptocurrency transactions. - Integration with various blockchain networks. - Strong in anti-money laundering.	Reliable digital forensics tool. - Capable of creating forensic images. - Broad support for various file systems.	Effective for extracting data from social media and web-based sources. - Useful for gathering contextual evidence.	Comprehensive forensic tool for various digital investigations. - Supports a wide range of file systems and devices.
Disadvantages	Expensive. - Requires subscription. - Limited to on-chain data analysis.	High cost. - Primarily focused on on-chain data. - Limited support for offline wallet data.	Primarily used for general digital forensics. - Limited cryptocurrency-specific analysis. - Requires manual analysis of extracted data.	Not specifically designed for cryptocurrency analysis. - Less effective for technical wallet data.	Expensive. - General-purpose tool with limited cryptocurrency-specific features. - Requires extensive training.
Comparison to CryptoInfoGetter	CryptoInfoGetter focuses on artifact analysis from Android devices. - Provides detailed information from hardware wallet apps, complementing on-chain data.	CryptoInfoGetter offers analysis of offline wallet artifacts, which CipherTrace does not cover. - More cost-effective for specific device-based investigations.	CryptoInfoGetter is specialized for cryptocurrency wallet artifacts. - Provides automated extraction and analysis, streamlining the process.	CryptoInfoGetter focuses on technical data from cryptocurrency wallets. - More suited for direct cryptocurrency forensic investigations.	CryptoInfoGetter provides targeted analysis for cryptocurrency wallets. - Simplifies and focuses on relevant data extraction, making it more accessible for specialized investigations.

3. ARITIFACT ANALYSIS

In our analysis, we utilized a rooted Samsung Galaxy S10 5G running Android 12, along with two prominent hardware wallets: the D'cent Biometric hardware wallet and the Ledger Nano S. To interface with these hardware wallets, we employed their respective Android-specific applications, D'cent Wallet for D'cent and Ledger Live for Ledger. Our investigation primarily centered on scrutinizing the database files generated within the /data/data/<package_name> path on the Android device, where we identified significant cryptocurrency-related data. Transactions were initiated using Bitcoin Testnet and Ethereum Testnet (ETH-GOERLI) to simulate real-world scenarios. The extraction and subsequent analysis of these database files were conducted within a Windows 10 environment, employing the Android Debug Bridge (ADB) tool for seamless file acquisition.

Table 1. Full Specifications of the devices used in the study

Device Type	Device Name	Version
Android	Galaxy S10 5G	Android 12
D'cent	D'cent Biometric hardware wallet	Kernel Version 2.25.2.83c3 KSM Version 1.0.0.1139
Ledger	Ledger Nano S	MCU Version 2.1.0 SE Version 1.12
PC	Windows 10 Pro	

The detailed specifications of the devices used are outlined in Table 2, encapsulating the Android device, hardware wallets, and the operating system utilized. Notably, the Galaxy S10 5G ran on Android 12, while the D'cent Biometric hardware wallet and Ledger Nano S boasted specific kernel and version details. The analysis was facilitated by the utilization of various tools and applications, as detailed in **Table 3**, which included D'cent Wallet, Ledger Live, and the Android Debug Bridge (ADB).

Table 2. Tools and Applications Used

Software Name	Version	Usage
D'cent Wallet	5.24.1	Android Application for D'cent Hardware Wallet
Ledger Live	3.20.1	Android Application for Ledger Hardware Wallet
Android Debug Bridge	33.0.3	Android File Acquisition

Delving deeper into the examination of the D'cent Wallet, identified through the package name com.kr.iotrust.dcent.wallet, we found that it stores its data within the default.realm file, residing in the files folder. This file contained a wealth of cryptocurrency-related information, including wallet details, hardware wallet specifics, and pending transactions. Notably, wallet labels and addresses served as vital indicators of usage intent and transaction histories, while hardware wallet data aided in pinpointing cold wallets owned by users, crucial for investigative purposes. Moreover, pending transaction details, accessible solely from the Android device and mempool, provided concrete evidence of transactions originating from the specific Android device, facilitating the creation of a timeline for transaction events.

The Ledger Live application, identified through the package name com.ledger.live, stored its data within the AsyncStorage file situated in the databases folder. This Key-Value database file primarily housed details regarding cryptocurrency wallets, hardware wallets, transactions, pending

transactions, and the application's initial execution date. Wallet labels were instrumental in discerning the purpose of usage, while hardware wallet information aided in identifying cold wallets, offering valuable insights for investigative endeavors. Unlike the D'cent Wallet, Ledger Live retained all transaction information within the database file, streamlining the process of constructing a timeline. Pending transaction details corroborated transactions originating from the specific Android device, furnishing precise transaction creation timestamps for timeline construction.

4. IMPLEMENTATION AND UTILIZATION OF THE TOOL

In this section, we detail the implementation and utilization of CryptoInfoGetter, a tool developed based on the artifact analysis results presented in Section previous of this paper. CryptoInfoGetter serves as a specialized solution for acquiring essential cryptocurrency-related data from Android devices connected to hardware wallets. Leveraging the insights gleaned from our analysis, we crafted CryptoInfoGetter using C++ within the Visual Studio 2019 environment, ensuring compatibility with the Windows operating system. To access and parse the realm file containing D'cent's application data, we integrated the open-source Realm Core library into our tool. Similarly, for extracting information from the AsyncStorage file housing Ledger's application data, we harnessed the capabilities of the open-source SQLite3 library.

Upon execution, CryptoInfoGetter offers a user-friendly interface, allowing forensic investigators to specify their desired extraction option - either '-dcent' for D'cent information or '-ledger' for Ledger information - via the command prompt (cmd). Additionally, users must provide the path where the files from the Android device are stored to initiate the extraction process seamlessly.

Once the extraction is complete, the acquired cryptocurrency data holds significant value for forensic investigations. Forensic analysts can cross-verify this data by querying the blockchain network for validity, thereby ensuring its reliability and integrity. This validated information serves as a cornerstone for constructing comprehensive crime timelines or serving as compelling evidence in legal proceedings. Notably, CryptoInfoGetter enables analysts to uncover potential criminal intent by analyzing data not directly recorded on the blockchain network, including wallet labels, pending transactions, and hardware wallet specifics. Moreover, the tool provides insights into users' patterns of hardware wallet usage, including details on the types and quantities employed, thereby enriching investigative efforts. CryptoInfoGetter emerges as a powerful asset for forensic analysts, offering a robust means to gather, verify, and utilize cryptocurrency-related data within the context of criminal investigations. By streamlining the extraction process and providing valuable insights, CryptoInfoGetter stands at the forefront of cryptocurrency forensic analysis, empowering investigators to unravel complex digital transactions and combat cryptocurrency-related crimes effectively. The specific data retrieved from the D'cent wallet application, including detailed information on wallet addresses, transaction histories, and hardware wallet configurations. The improved background in the figure enhances visibility, allowing for a clearer interpretation of the extracted data, shown in Figure 1. The data extracted from the Ledger wallet application, providing insights into the wallet details, transactions, and pending transactions. The enhanced background of this figure ensures better visualization and understanding of the information retrieved from the Ledger wallet, shown in Figure 2.

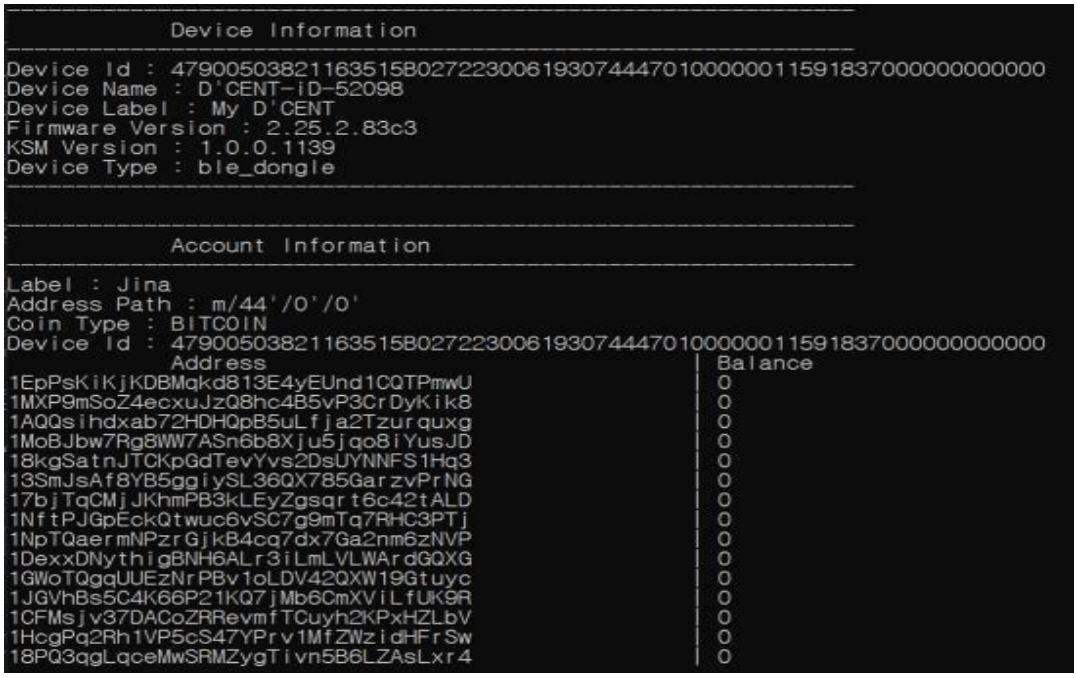

Figure 1. Illustrates the execution outcome of CryptoInfoGetter with the D'cent option.

Figure 2. Depicts the execution result of CryptoInfoGetter with the Ledger option.

5. DISCUSSION

Our artifact analysis offers significant insights into the realm of cryptocurrency transactions conducted via Android devices connected to hardware wallets. By scrutinizing the data generated by the D'cent Biometric Wallet and Ledger Nano S, we've uncovered valuable information crucial for forensic analysis and the investigation of cryptocurrency-related crimes. The findings underscore the forensic significance of artifact analysis, providing forensic analysts with a treasure trove of data including wallet details, transaction histories, and hardware wallet configurations, pivotal for tracing fund flows and identifying transaction participants. However, this analysis also illuminates challenges such as the dynamic nature of cryptocurrency transactions and the inherent anonymity features, which complicate accurate tracking and attribution. Despite these challenges,

our study highlights opportunities for enhancing investigative techniques and developing specialized tools tailored to the forensic analysis of cryptocurrency transactions. Crucially, ensuring the validity and reliability of the obtained data remains paramount, necessitating cross-verification through blockchain network queries to corroborate extracted information. Ethical and legal considerations loom large, demanding adherence to ethical guidelines, data protection laws, and privacy concerns to safeguard the integrity and admissibility of forensic findings in legal proceedings. Looking ahead, future research should focus on addressing emerging challenges, advancing investigative methods, and exploring the impact of evolving technologies like decentralized finance (DeFi) and non-fungible tokens (NFTs) on forensic practice. Collaboration among researchers, law enforcement agencies, and industry stakeholders will be instrumental in advancing the field of cryptocurrency forensic analysis and countering evolving threats in the digital landscape.

Our artifact analysis offers significant insights into the forensic investigation of cryptocurrency transactions facilitated through Android devices connected to hardware wallets. Beyond the primary challenge of tracing transactions back to their originators, several other critical issues impact the effectiveness of cryptocurrency forensics. Data integrity and accuracy remains a fundamental concern. Ensuring that the data extracted from Android devices and hardware wallets is both accurate and unaltered is crucial for reliable forensic analysis. Artifacts can be prone to modification or corruption, which may lead to erroneous conclusions. To mitigate this, forensic tools must undergo rigorous validation processes to confirm their reliability and accuracy in data extraction.

Data encryption and obfuscation further complicate forensic investigations. Many cryptocurrency wallet applications employ sophisticated encryption and obfuscation techniques to protect user data, creating barriers to accessing and interpreting this information. Forensic analysts must develop and apply methods to effectively bypass or decrypt such data while maintaining its integrity, which requires advanced technical skills and tools. Volume and complexity of data is another significant challenge. Cryptocurrency transactions generate vast amounts of data, often involving multiple wallets and addresses. Analyzing this data to extract relevant information can be overwhelming and complex. Effective data management strategies and analytical techniques are essential to handle and sift through the large volumes of data efficiently.

Evolving technologies in the cryptocurrency sector introduce additional difficulties. The continuous development of new wallet types, blockchain protocols, and decentralized finance (DeFi) platforms means that forensic tools and methodologies must constantly adapt to accommodate novel data structures and transaction formats. Staying updated with technological advancements is critical for maintaining effective forensic practices.

Jurisdictional and legal issues present another layer of complexity. Cryptocurrency transactions frequently span international borders, leading to varied regulations across different jurisdictions. This variability can create legal challenges for forensic investigations, affecting the admissibility of findings in court. Navigating these legal complexities requires careful consideration of international laws and regulations.

6. CONCLUSION

Our investigation into the forensic analysis of cryptocurrency transactions conducted via Android devices connected to hardware wallets has illuminated critical facets of this complex digital ecosystem. Through meticulous artifact analysis and the development of the CryptoInfoGetter tool, we have unveiled a wealth of data pertaining to

wallet details, transaction histories, and hardware wallet configurations. These insights serve as invaluable assets for forensic investigators, offering a pathway to trace fund flows, identify transaction participants, and ultimately unravel the intricate web of cryptocurrency-related crimes.

While our study has shed light on the forensic significance of artifact analysis, it has also underscored the multifaceted challenges inherent in investigating cryptocurrency transactions. The dynamic nature of these transactions, coupled with the anonymity features embedded in cryptocurrencies, presents formidable hurdles for forensic analysts. However, we remain optimistic about the opportunities for innovation and advancement in this field.

Looking ahead: in navigating the evolving landscape of cryptocurrency forensic analysis, paramount importance will lie with collaboration among researchers; law enforcement agencies and industry stakeholders. Through fostering partnerships--and sharing expertise—we can address emerging challenges collectively, develop cutting-edge investigative techniques and bolster the efficacy of forensic tools. Our endeavors must always prioritize ethical and legal considerations. Delving deeper into cryptocurrency forensic analysis necessitates us to maintain stringent ethical guidelines, adhere to data protection laws, and respect individual privacy rights. We can ensure the integrity and admissibility of our forensic findings in legal proceedings by upholding impeccable standards of ethical conduct..

Our study represents a significant step forward in the field of cryptocurrency forensic analysis. By leveraging the insights gleaned from artifact analysis and embracing a collaborative approach, we can fortify our efforts to combat cryptocurrency-related crimes and uphold the integrity of digital transactions in an increasingly interconnected world.

REFERENCE

Aiolli, F., Conti, M., Gangwal, A., & Polato, M. (2019). Mind your wallet's privacy: Identifying Bitcoin wallet apps and user's actions through network traffic analysis. Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing, 1484–1491. https://doi.org/10.1145/3297280.3297430

Dmitrienko, A., Noack, D., & Yung, M. (2017). Secure Wallet-Assisted Offline Bitcoin Payments with Double-Spender Revocation. Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security, 520–531. https://doi.org/10.1145/3052973.3052980

He, D., Li, S., Li, C., Zhu, S., Chan, S., Min, W., & Guizani, N. (2020). Security Analysis of Cryptocurrency Wallets in Android-Based Applications. IEEE Network, 34(6), 114–119. https://doi.org/10.1109/MNET.011.2000025

Khan, A. G., Zahid, A. H., Hussain, M., & Riaz, U. (2019). Security Of Cryptocurrency Using Hardware Wallet And QR Code. 2019 International Conference on Innovative Computing (ICIC), 1–10. https://doi.org/10.1109/ICIC48496.2019.8966739

Mirza, D., & Rahulamathavan, Y. (2023). Security Analysis of Android Hot Cryptocurrency Wallet Applications. In C. Hewage, Y. Rahulamathavan, & D.

Ratnayake (Eds.), Data Protection in a Post-Pandemic Society (pp. 79–111). Springer International Publishing. https://doi.org/10.1007/978-3-031-34006-2_3

Mirza, M. M., Ozer, A., & Karabiyik, U. (2022). Mobile Cyber Forensic Investigations of Web3 Wallets on Android and iOS. Applied Sciences, 12(21), 11180. https://doi.org/10.3390/app122111180

Qi, M., Xu, Z., Jiao, T., Wen, S., Xiang, Y., & Nan, G. (2022). A Comparative Study on the Security of Cryptocurrency Wallets in Android System. 2022 IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 399–406. https://doi.org/10.1109/TrustCom56396.2022.00062

Saeed Rasheed, R., Hamdi Ateyeh Al-Shqeerat, K., Salah Ghorab, A., Salama AbuOwaimer, F., & Ahmed AbuSamra, A. (2023). Blockchain Mobile Wallet with Secure Offline Transactions. Computers, Materials & Continua, 75(2), 2905–2919. https://doi.org/10.32604/cmc.2023.036691

Suratkar, S., Shirole, M., & Bhirud, S. (2020). Cryptocurrency Wallet: A Review. 2020 4th International Conference on Computer, Communication and Signal Processing (ICCCSP), 1–7. https://doi.org/10.1109/ICCCSP49186.2020.9315193

Thomas, T., Piscitelli, M., Shavrov, I., & Baggili, I. (2020). Memory FORESHADOW: Memory FOREnSics of HArDware CryptOcurrency wallets – A Tool and Visualization Framework. Forensic Science International: Digital Investigation, 33, 301002. https://doi.org/10.1016/j.fsidi.2020.301002

Uddin, M. S., Mannan, M., & Youssef, A. (2021). Horus: A Security Assessment Framework for Android Crypto Wallets. In J. Garcia-Alfaro, S. Li, R. Poovendran, H. Debar, & M. Yung (Eds.), Security and Privacy in Communication Networks (Vol. 399, pp. 120–139). Springer International Publishing. https://doi.org/10.1007/978-3-030-90022-9_7