[1] Adrian Hartanto *
[2] Ivan Sebastian Edbert
[3] Putri Sanggabuana Setiawan

Exploring the Implementation of Hierarchical Deterministic Wallets in Organizational Settings

Journal of Electrical Systems

Abstract: - Several studies have delved into technical aspects of Hierarchical Deterministic wallets. However, there is yet research regarding its use in organizations. This study aims to explore various aspects of HD wallets in organizational settings. Exploring technical requirements for implementation, benefits and risks of adoption for organizations, and adoption recommendations. The data will be gathered through a systematic literature review, utilizing specific coding forms to extract information from different literatures. Furthermore, an experimental implementation for gathering information regarding technical requirements of HD wallets. The results of the review aim to answer the research questions constructed prior to the start of the research, covering the possible benefits and risks of adopting HD wallets, technical specifications, and considerations of adoption. In the end, a literature review was conducted on 18 literatures, and an implementation was created uncovering information regarding technical aspects of implementing HD wallets, such as access control, key management, data transmission, and more. The findings provided information regarding the requirements and considerations relating to the implementation and adoption of HD wallets. Providing several recommendations for organizations looking to adopt HD wallets, such as conducting regular security audits, human factors, and key management practices.

Keywords: Blockchain, Cryptocurrency, Hierarchical Deterministic Wallet, HD Wallet, Organizational Implementation.

I. Introduction

In cryptocurrencies, the whole structure fundamentally revolves around the concept of cryptographic key pairs for coin or account ownership. A keypair containing a private and public key is used to prove ownership of and conduct transactions with holder's funds, a holder being one that actually has ownership of the funds [1]. In practical terms, transferring funds involves the sender (in this case holder) signing a transaction using their private key, with the blockchain subsequently verifying the transaction's signature through the sender's public key. And once confirmed, this transaction is now irreversible, unlike the more traditional bank transfer system. From a privacy and security standpoint, a problem arises if a single keypair was repeatedly used for multiple transactions. The repeated utilization of a single key elevates the risk of exposure to attacks, being publicly available, the key becomes an appealing target for an attack for adversaries [2]. To prevent exposure and mitigate attacks, a person may create multiple keys, using different keys for different transactions. But this raises another issue regarding key management, where too many keys are generated, resulting in an increase in difficulty for the management of keys [3]. In response to this key management dilemma, a practical solution has emerged in the form of Hierarchical Deterministic (HD) wallets.

Hierarchical Deterministic Wallets or more commonly called HD wallets, a concept introduced and proposed in BIP32 in 2012 [4], has captivated both individuals and organizations that seek to increase security, privacy and flexibility in managing funds and assets. While the adoption and research on HD wallets are intensifying, the organizational integration of side remains an understudied and crucial domain to explore. HD wallets evolved as a more advanced version of deterministic wallets, that introduces a hierarchical structure and simplifies the process of key creation and retrieval. Presently, HD wallets are widely acknowledged as the standard within the Bitcoin community and numerous other cryptocurrencies that are either in the process of implementing or have already incorporated HD wallets [4]. HD wallets provide a more convenient way of generating different keypairs from master keys (master private and public key) and a chaincode [5]. Utilizing the master private key, master public key and an index, the i-th derived private key can be generated [6]. Similarly, the corresponding public key of the derived private key can be retrieved through the concatenation of the master public key, the hash of the master public key and index, and the generator of the ECDSA algorithm [3], [6].

[1] Student, Computer Science Department, School of Computer Science, Bina Nusantara University, Jakarta, Indonesia. adrian.hartanto008@binus.ac.id
[2] Assistant Professor, Computer Science Department, School of Computer Science, Bina Nusantara University, Jakarta, Indonesia. ivan.edbert@binus.ac.id
[3] Lecturer, Computer Science Department, School of Computer Science, Bina Nusantara University, Jakarta, Indonesia. putri.sanggabuana@binus.ac.id
* Corresponding Author Email: adrian.hartanto008@binus.ac.id

In today's technological landscape, the integration of blockchain technology by organizations or businesses emerged as a critical topic to discuss. As blockchain offers better transparency, security and efficiency in handling both transactions and data, its adoption by businesses may offer various advantages. Thus, the significance of managing cryptographic keys within this framework cannot be overstressed. Proper security measures and potential security issues must first be addressed. To utilize deterministic wallets securely, other than keeping the private key safe and unknown, other keys must also be kept safe and hidden [6]. Due to known issues regarding vulnerabilities in the signing algorithms or possible collusion, not only does the private key need to be kept hidden, but also all derived private keys. Current existing implementations of HD wallets have admitted to having an existing exploit, where an attacker may recover the master private key given a master public key and a non-hardened child private key [4], [6]. Initially this vulnerability was discovered by the creator of BIP32, and it compensates by enabling hardened-keys generation [7]. Unfortunately, utilizing hardened keys loses the master public key property.

This study aims to explore the potential implementation of hierarchical deterministic wallets for the main purpose of managing organizations' financials. Where this study will explore and analyze existing HD wallet standards, such as BIP32 and BIP44, and proposed implementations by researchers. Furthermore, this study will also propose recommendations for implementing HD wallets in organizations, such as possible adoption challenges, integration recommendations and practical considerations. Moreover, this study also creates an HD wallet implementation, providing a clearer picture on certain technical requirements of implementing HD wallets for organizations. The overall objective of this study is to give a better understanding of the functionality of HD wallets and the risks involved in adopting this technology in organizations. This study may have the capacity to act as an educational tool for individuals and organizations keen on adopting HD wallets. It has the potential to contribute to existing knowledge and facilitate the connection between theoretical ideas and practical implementation of HD wallets.

II. Literature Review

Hierarchical Deterministic wallet is a key generation technique used in many famous cryptocurrencies, such as bitcoin. Defined in the BIP32 standard, HD wallets can be referred as a type-2 wallet and forms a tree-like structure, generating keys through the use of previous parent keys [8]. An implementation flaw of HD wallets exists in the form of the ability for adversaries to derive the master private key through preemptively knowing the master public key and any child derived key [9]. This attack is known as privilege escalation attacks, where adversaries may gain higher unauthorized access. To mitigate this vulnerability, BIP32 proposes a hardened version of the keys, but this hardened solution makes key management more difficult, and auditing requires access to more keys [10].

A. Proposed Implementations of HD Wallets

In an attempt to solve the previous flaw, many researchers have proposed their implementation models of HD wallets, some claiming to be secure against privilege escalation attacks by utilizing other cryptographic concepts. An implementation proposed by Xin Yin et al. [4], combines the virtues of both hierarchical deterministic wallets and stealth addresses technology simultaneously or referred to as HDWSA (Hierarchical Deterministic Wallet Stealth Address). HDWSA maintains the capabilities of the main properties of HD wallets (deterministic generation, master public key and hierarchical property) whilst also solving the issue of the treasurer-auditor issue, which is essentially privilege escalation attack, through the use of stealth address and creation of a private view and spend key. Similar to the previous research, research conducted by Zhen Liu et. al. [11] introduces and formalize a new signature variant called Key-Insulated and Privacy-Preserving Signature Scheme with Publicly Derived Public Key. This new signature variant claims to provide the capabilities of deterministic wallets and stealth addresses, whilst removing the inherent vulnerabilities. Along with the signature variant, the research also provides a secure and efficient construction to serve as a reliable method to build privacy-preserving cryptocurrencies. These two researches similarly combine the virtues of HD wallet with Stealth Addresses, proving the security of their implementation security.

Another research by Adriano Di Luzio et al. [12], proposed an interesting implementation of HD wallets, named Arcula. Arcula is a system based on a well-known cryptographic technique called Hierarchical Key Assignment or HKA, which allows management of complex hierarchical structures that require flexible access control. In the research, they claim that inherently, their model is designed to be secure against privilege escalation attacks. Additionally, aiming to reduce the vulnerability to privilege escalation attacks, research conducted by Gus Gutoski and Douglas Stebila [7] introduced an innovative HD wallet implementation. This design can endure the compromise of m-private keys without affecting the size of the master private key through the use of the Threshold

Signature Scheme or TSS. The proposed solution addresses the treasurer-auditor dilemma by incorporating a higher number of private keys (m) compared to the number of departments (t). Similarly, research by ChihYun Chuang et al. [13], proposes a dual-computation system for generating the master keys, hardened keys, or any other derived child keys. Utilizing a protocol called DualEx, a two-party secure computation system. The primary purpose of this research is to design a BIP32 compliant protocol that enables Threshold Signature.

B. *Adoption of Cryptocurrency in Organizations*

To understand the potential utilization of HD wallets or any other cryptocurrency technologies in organizations, several studies have conducted research on factors that play a role in the adoption of cryptocurrency. A study by Benanni, K. S. and Arpaci I. conducted in 2022 [14], attempts to answer this very question. The study's main objective is to discover the factors influencing individual and organizational adoption of cryptocurrencies, utilizing the Innovation Diffusion Theory (IDT) model at an individual level and the Technology-Organization-Environment (TOE) framework for the organization level. In the context of organizational adoption, the study states several factors separated to three main categories, mainly Technological, Organizational, and Environmental factors. Similar to the previous study, another study by Alzahrani S. and Daim T. in 2019 [15], investigates factors influencing the adoption decision of cryptocurrencies. Conducting a literature review and differing slightly in terms of categorical factors that influences adoption, the study found Technical, Economic, Social, and Personal to be the four main factor categories. Where factors that most influence the adoption of cryptocurrencies being, investment opportunities, anonymity of users, user technological curiosity, speed of transaction, low cost, and acceptance by established businesses.

C. *Security of HD Wallets*

On the context of the security of HD wallets' implementation, several studies were conducted covering the standards and cryptographic primitives behind HD wallets. Research by Poulami Das et al. [5] has looked into the security aspects of BIP32, a widely used HD wallet standard known as Bitcoin Implementation Proposal 32. This study discusses the security limitations of HD wallets, examining the use of hot/cold wallet systems for BIP32 HD wallets. It also suggests a tweak to the implementation by rerandomizing the ECDSA algorithm. Another research by the same authors, Poulami Das et al. [16] presents a secure (t, n)-threshold signature system for hierarchical deterministic wallets, spreading non-hardened wallets across n devices to improve security against compromises. This method is particularly useful for strengthening the security of different wallet types in blockchain applications. Moreover, the research suggests a creative solution utilizing a threshold verifiable random function (TVRF) for effective computation of pseudorandom values in hardened node derivation, addressing issues of communication overhead while upholding security. Another study conducted by Jens Groth and Victor Shoup [17] performed a security analysis of the ECDSA algorithm and its variations, such as ECDSA with additive pre-signatures and additive key derivation. Furthermore, this study also delves into the key derivation function (KDF) utilized in BIP32.

III. METHODOLOGY

To thoroughly study how Hierarchical Deterministic Wallets (HDWs) are used in organizational settings, using a method that focuses on combining existing research and standards, one example is BIP32 that relates to the current implementation of HD wallets in Bitcoin [18]. This section explains how this study systematically analyze a wide range of literature and standards about HD wallets. This method helps us get a complete picture of the problems, risks, and best practices linked to using HD wallets in organizations. Additionally, this study also creates an implementation of HD wallets. This implementation would act as an example of important aspects and requirements necessary for utilizing HD wallets, specifically in organizational settings.

A. *Data Collection and Analysis*

In regard to the collection of data, this study will employ a secondary data analysis methodology and systematic literature review, focusing on published literature relevant to the topic of this study. Secondary data analysis involves analyzing data synthesized by previous studies to answer new or different questions on a similar topic [19]. To gain a comprehensive understanding of the technology and concepts underpinning hierarchical deterministic wallets, this study will conduct a systematic literature and document review, synthesizing information from academic articles, research studies, standards, and relevant proposals. The specific details of the systematic literature review process will be covered in the next section.

B. Systematic Literature Review Process

The overall process of literature and document review would be conducted systematically, covering 7 general steps and reiteration of the process if deemed necessary [20]. The first step is formulating research questions relevant to the topic of this study, these research questions act as the basis of the literature review. The research questions in this study cover aspects of HD wallets and its implementation in organizational settings, which includes:

1) What are the benefits and risks of utilizing HD wallets?
2) What are the technical requirements necessary for implementing HD wallets designed for organizations?
3) What considerations should organizations keep in mind when adopting HD wallets?

The second step is selecting and validating the review protocol, this involves determining important aspects of the review process. This study aims to explore aspects relating to the implementation of HD wallets in organizational settings. To accomplish this goal, a literature review will be conducted with the inclusion criteria including research journals, studies, or other official literatures generally relating to Hierarchical Deterministic wallets or deterministic wallets in general. This study only includes studies written in English. Furthermore, to conduct this literature review the keywords used are "Hierarchical Deterministic Wallet", "Bitcoin Wallets", "BIP32 wallets", "Hierarchical Deterministic wallets for organizations", and "HD wallets security" searched primarily through Google Scholar, IEEE Xplore, and ACM Digital Library.

In the following third step, the search for relevant literature through electronic databases begins. Where the fourth step involves assessing the inclusion of found literature based on previously determined criteria. Subsequently, the fifth step involves extracting data from the literatures, conducted using coding forms containing the specific types of data to be extracted from the literatures [21]. Due to the varying types of literature that might be collected, this study decided on categorizing the literatures based on their research objectives and create specific coding forms for each category, which are studies proposing implementation or schemes, studies conducting analysis, and BIPs. The common sections between all categories include the general information of the literature, its main focus, mentions of HD wallets risks and/or benefits, technical requirements, and any other additional information. Furthermore, for studies proposing new implementations or schemes there are two main sections discussing the proposed implementation or schemes and the benefits or advantages of each. For studies conducting analysis, the coding forms include the method each literature used to do the analysis and detailed description of each literature (focus, impact and findings). Finally, for Bitcoin Implementation Proposals, the literature review will focus on the proposed changes in the BIP, covering the scope, focus and features introduced in each. Following data extraction, data from the literatures are then analyzed and synthesized to identify common stereotypes through textual description or charts to draw conclusions and address previously determined research questions [20]. Depending on the insights gained from the previous step, it may be necessary to revisit and refine the research questions, leading to a reiteration of the process. Finally, if no reiteration of the process is required, the findings and process of the review are reported and explained.

C. Implementation of HD Wallets

Based on knowledge obtained from the literature review, this study also implements a HD wallet, specifically for organizational use cases. This implementation of HD wallets draws important information regarding crucial aspects to consider when utilizing HD wallets in organizational settings. This implementation functions as a custodial wallet that stores the organization's keys in an encrypted state within a database managed by the organization themselves. Regarding the platform of the implementation, this study decided on creating a web-based wallet that performs private actions in the backend. The web-based client was built using the NextJS frontend framework, the web server was built using Express and Nodejs, whilst MySQL is the chosen database for this implementation. The wider architecture of the implementation involves several other components, which are AWS KMS and Blockcypher. In the implementation, AWS KMS is utilized as an encryption tool in storing the master keys in the database, this acts as an extra layer of security to protect the keys in the event of a data breach. Furthermore, integration to the bitcoin blockchain itself is required, thus this study decided on incorporating the use of Blockcypher's API services. The relationship between these components is visualized in Figure 1.

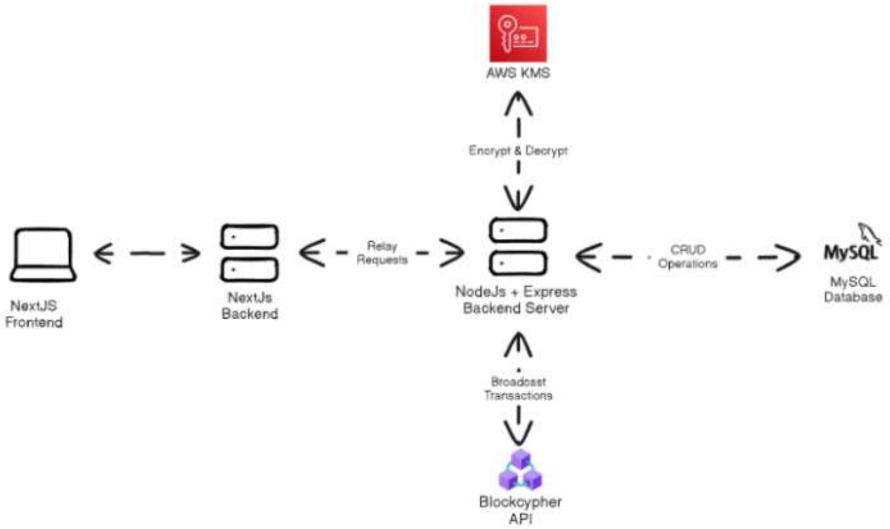

Figure 1. Architecture of HD Wallet Implementation

Initially, when constructing the objectives and requirements of the system, one aspect this study wanted to achieve, regarding the implementation, was to enable hierarchical control over the wallet. To achieve this functionality, a role-based access system enables hierarchical control over addresses and accounts. Additionally, to mitigate risks like key leakage and potential privilege escalation attacks, the system ensures that both public and private keys remain undisclosed. Instead, members or users are given access to the addresses of the wallets assigned to them. Actions such as key derivation and signing transactions are always conducted in the backend server, away from members or users. Further specifications regarding techniques or concepts utilized by the system will be discussed in the fourth section.

D. Possible Limitations of Research

While exploring the implementation of HD addresses, it's important to recognize some limitations in how this research is conducted. To start, there may not be abundant detailed information accessible about these cryptographic concepts. Despite efforts to examine all pertinent literature, there is a scarcity of scholarly articles, industry reports, or standardized documents specifically dedicated to the discussion of HD wallets. This scarcity could constrain the depth of understanding of these topics, potentially leading to a gap in overall knowledge.

IV. Results and Discussion

To explore different aspects of the integration of HD wallets, this study reviewed several relevant literatures relating to Hierarchical Deterministic Wallets or deterministic wallets in general. During the search for literature, initial iteration of the search resulted in 14 pieces of literature being found, covering topics related to HD wallets or deterministic wallets in general. Where after later iterations, 4 more relevant literature were found. These literatures include studies proposing implementations, security analysis, Bitcoin Implementation Proposals (BIPs), and standard proposal documents. For instance, a study covering the security reduction of BIP32 wallets [5] or a study proposing an implementation of HD wallets with Stealth Address [4]. Furthermore, literatures relating to the implementation of Bitcoin (pioneers of HD wallets) called BIPs [18], [22], [23], covers a wide range of topics, where it may cover technical improvements or perhaps protocol changes of the Bitcoin network. The following three sections will convey the results of the research conducted and how it answers the research questions constructed prior to the start of the research.

A. The Benefits and Risks of Utilizing HD wallets

Hierarchical Deterministic wallets enable many use cases and applications, tackling the financial requirements of organizations or institutions. This section will focus on the possible applications of HD wallets, exploring sectors where utilization of HD wallets may increase the efficiency, security, and convenience of organizing financial transactions. From a wider perspective, HD wallets are perfect for organizations, due to their hierarchical nature. Enabling more practical key management and assignment for each department in the organizations, whilst providing simpler backup and recovery processes [7]. Furthermore, the master public key property allows trustless auditing capabilities, where third-party auditors may derive relevant public keys using only the master public key and no further information [4], [12]. Additionally, another use case of HD wallets is e-commerce transactions. HD wallets enable easier generation of cold addresses, which is especially important in e-commerce, where it requires receiving funds from customers [12]. Finally, a simpler use case for HD wallets is for crafting brain wallets or low-maintenance wallets, which is enabled through the use of mnemonics to regenerate the whole tree.

On the other hand, utilization of HD wallets does come with several risks and challenges. Perhaps one of the more well-known attacks is privilege escalation, an attack allowing an adversary back-tracking the master private key by only knowing the master public key and a child derived key [4], [7]. Although a solution for this vulnerability was proposed in the form of hardened keys, this solution loses the master public key property. Furthermore, having only a single master key introduces a potential single point of failure. This may potentially lead to a complete loss of funds, if no proper storage and security measures are in place. Software implementation flaws may also cause vulnerabilities, attacks such as man-in-the-middle or identity spoofing [24] Causing unauthorized access to sensitive information, namely private/public keys, derivation paths, or user data.

B. HD Wallet Implementation Technical Specification

The implementation created for this study mainly focuses on implementing HD wallets for organizational use cases. Where the main objective throughout the creation process is to explore implementation options regarding the security and performance side of HD wallets. This section will provide information and specifics regarding the technical decisions undertaken throughout the development process. As previously outlined, the wallet is a custodial wallet, where members' addresses and keys are managed by the wallet. The wallet itself is a web-based application that communicates with an express server, where crucial operations are conducted server-side.

In developing the implementation, several technical decisions are worth noting. Access control of the application was the first undertaking throughout the development process, as a role-based access control system is deployed. There being three roles, an admin, department head, and member. These three roles hold different capabilities, an admin being the highest-ranking role, having the ability to create accounts to deriving addresses for lower roles. To enhance security, users must set up two-factor authentication, employing Time-based One-Time Passwords (TOTPs), which ensures account security even if passwords are compromised. Furthermore, department heads are part of a department, having control over their own department. Being able to create accounts, derive child wallets, and assign them to members within the department, ensuring compartmentalization.

Additionally, considerable consideration was given to wallet derivation paths, to comply with existing standards such as BIP44 [22]. Figure 2 illustrates the established derivation paths in the implementation. The department index corresponds to the account level in BIP44, employing hardened derivation, while individual members utilize addresses from the address index level. To provide an illustration what was implemented, say there is a department called IT with a department ID of 1. Thus, the path for the department head's wallet would be *"m/44'/0'"*. Furthermore, the address for members would be *"m/44'/0'/0/1"*.

m/44'/0'/**{department_index}**'/**{change}**/**{member_index}**

Figure 2. Established Wallet Derivation Path Format

For the creation and derivation of the wallets, the implementation utilized the "bitcoinjs-lib" Javascript/Typescript library for NodeJS. The library itself has mentioned that it uses the "tiny-secp256k1" elliptic curve. The storage of the keys is another important aspect considered, throughout the research process, several secure methods are recommended. The most relevant one suggesting the use of offline/cold wallets to store important keys, such as Hardware Secure Modules or HSMs.

Regardless, for this implementation, this study decided on utilizing AWS KMS to encrypt relevant keys before storing them in the MySQL database. To prevent any potential loss or leaks of any private or public keys, no keys are exposed even to the users owning each key. Activities conducted utilizing the keys are done automatically in the backend in a secure environment and is not handled directly by each user. Thus, at no point does sensitive information get exposed in an unsecure environment.

Furthermore, throughout activities of the system, it is imperative that no sensitive information such as signatures, including public ones, are transmitted through unsecure channels of communication. Regardless, due to the sensitive nature of the information, communication between components requires a certain standard of security. Thus, HTTPS is utilized for encrypting data transmission between the frontend client to the backend server.

Moreover, another key aspect of the implementation is its approach to conducting and constructing transactions. Here, a multi-signature scheme is employed, utilizing P2SH addresses. The multi-signature scheme requires signatures, employing a 2-of-3 multi-signature scheme. For security purposes, only the owner of a wallet can initiate a transaction, and each transaction will require signatures from superiors. This ensures a level of verification and accountability for each transaction, tying each to addresses or keys. The signing process in this implementation is done locally, utilizing Partially Signed Bitcoin Transaction (PSBT)[23], meaning keys or signatures never leave the secure server. After signing is complete, it will then finalize all inputs and broadcast the finished transaction using the Blockcypher API, awaiting block confirmations.

C. Considerations for Adopting HD Wallets

This section will discuss several insights gained from the implementation this study created, to better understand considerations for adopting HD wallets. The first point of discussion is key management, specifically key storage, in the implementation a simpler approach was employed. Choosing to store the keys in an encrypted state locally in the database, utilizing AWS KMS for symmetric encryption prior to storage. In a real-world scenario, other options exist regarding key storage, typically encompassing an offline storage of keys or even threshold cryptography techniques. Threshold cryptography techniques involve splitting the key into several pieces and storing them in separate locations, achieving enhanced resiliency against data breaches or unauthorized access [9]. Another storage option is to use Hardware Secure Modules or HSMs for managing the private keys and generating signatures [24]. Utilizing HSMs may improve resiliency of custodial systems, and better protect them from loss of private keys. Utilization of HSMs adds a new layer of security to the system, providing a secure storage for cryptographic keys, rendering no possible methods of externally accessing them. HSMs protect stored keys from manipulation attempts, whilst providing strong authentication mechanisms [25]. Moreover, key rotation is also an important aspect of key management, especially for organizations with high volumes of transactions. Employing multi-signature schemes requires key rotation to involve creating transactions, which may incur extra transaction fees and leak information. To avoid this, threshold signature schemes may be used instead, providing an off-chain option for access-control [24]. Key rotation in HD wallet specifically can be conducted in regards to rotating the child keys after every specific period depending on the volume of the transactions made.

Transaction and address types are also a factor to consider, this implementation utilizes P2SH transactions, creating a multi-signature setup. One downside of this decision is the large size of transactions for a multi-signature setup, which may increase fees when conducting transactions. Regardless, a multi-signature setup introduces an extra security measure for allocation and usage of funds. Whilst also introducing a level of accountability for the system, which is the main reasoning behind the decision to use multi-signatures. However, to reduce the amount of fees a user needs to pay, a wallet may construct SegWit transactions that reduces bandwidth requirements and consequently less fees [24]. Additionally, to protect the privacy of organizations, it is recommended to utilize private blockchain networks instead of public ones. This enables control of access on who can access the network, which leads to better privacy and control for organizations. Furthermore, due to the sensitivity of the data being processed, a tight identity verification process needs to be employed. In the current implementation, identity verification of each user involves a username, email, and password only. This can be further improved using two-factor authentication capabilities, such as Time-Based One-Time Passwords or Biometrics (Face or Fingerprint scans).

To access the implementation of HD wallet created for this study, the following is the GitHub link to the public repository https://github.com/Adrian-py/FortifyWallet.

V. Conclusion

Utilization of HD wallets introduce many virtues, which is especially beneficial for organizations looking to adopt this technology. Nevertheless, certain risks and challenges do exist throughout the process in adopting HD wallets, such as implementation flaws of HD wallets or security considerations. In the first stage of this study, a literature review was conducted, exploring aspects of HD wallets relating to its technical to possible applications. The literature review yielded approximately 18 literatures relating to HD wallets, from where this study was able to receive information regarding the applications of HD wallets to technical requirements for developing an implementation. The main objective behind the creation of the HD wallet implementation, was to provide insight regarding requirements for developing HD wallets specifically suited for organizations. In the end, the implementation provided lessons, regarding key management, transaction building, and other technicalities essential for an HD for organizations.

For organizations looking to adopt HD wallets, there are several recommendations this study can provide based on the findings of the literature review and implementation experiment. Regarding the utilization of HD wallets, it is important to consider the risks of incorporating HD wallets. For instance, it is important to consider the key management strategy to avoid the possible vulnerability of privilege escalation and to avoid a single point of failure in the form of the master private key. This can be achieved through establishing a secure key rotation protocol, enabling detailed logging, and enhancing backup capabilities. Furthermore, when planning to implement an HD wallet to be used, it is important to consider the technical requirements of the system. Important security measures need to be deeply considered, such as the storage and operation of keys (with HSMs being the best option), scalability, and system access controls. Regular security audits are also essential to identify and mitigate any flaws or vulnerabilities in the implementation. Finally, the human factor plays a significant role in successfully adopting a technology. Comprehensive training and awareness programs should be conducted to prevent any human errors. These recommendations may serve as further considerations for organizations looking to adopt HD wallets in their operations.

Acknowledgement

I would like express my gratitude to my thesis supervisors Ivan Sebastian Edbert and Putri Sanggabuana Setiawan for providing support and guidance throughout the research process, through review processes, recommendations, or other forms of guidance.

References

[1] H. Rezaeighaleh and C. C. Zou, "Deterministic sub-wallet for cryptocurrencies," in *2019 IEEE International Conference on Blockchain (Blockchain)*, IEEE, 2019, pp. 419–424.

[2] P. Das, S. Faust, and J. Loss, "A formal treatment of deterministic wallets," in *Proceedings of the 2019 ACM SIGSAC conference on computer and communications security*, 2019, pp. 651–668.

[3] H. Rezaeighaleh and C. C. Zou, "New secure approach to backup cryptocurrency wallets," in *2019 IEEE Global Communications Conference (GLOBECOM)*, IEEE, 2019, pp. 1–6.

[4] X. Yin, Z. Liu, G. Yang, G. Chen, and H. Zhu, "Secure hierarchical deterministic wallet supporting stealth address," in *European Symposium on Research in Computer Security*, Springer, 2022, pp. 89–109.

[5] P. Das, A. Erwig, S. Faust, J. Loss, and S. Riahi, "The exact security of BIP32 wallets," in *Proceedings of the 2021 ACM SIGSAC conference on computer and communications security*, 2021, pp. 1020–1042.

[6] N. Alkeilani Alkadri *et al.*, "Deterministic wallets in a quantum world," in *Proceedings of the 2020 ACM SIGSAC Conference On Computer And Communications Security*, 2020, pp. 1017–1031.

[7] G. Gutoski and D. Stebila, "Hierarchical deterministic bitcoin wallets that tolerate key leakage," in *International Conference on Financial Cryptography and Data Security*, Springer, 2015, pp. 497–504.

[8] E. Zaghloul, T. Li, M. W. Mutka, and J. Ren, "Bitcoin and blockchain: Security and privacy," *IEEE Internet Things J*, vol. 7, no. 10, pp. 10288–10313, 2020.

[9] S. Houy, P. Schmid, and A. Bartel, "Security Aspects of Cryptocurrency Wallets—A Systematic Literature Review," *ACM Comput Surv*, vol. 56, no. 1, pp. 1–31, 2023.

[10] N. T. Courtois, P. Emirdag, and F. Valsorda, "Private key recovery combination attacks: On extreme fragility of popular bitcoin key management, wallet and cold storage solutions in presence of poor RNG events," *Cryptology ePrint Archive*, 2014.

[11] Z. Liu *et al.*, "Secure deterministic wallet and stealth address: Key-insulated and privacy-preserving signature scheme with publicly derived public key," *IEEE Trans Dependable Secure Comput*, vol. 19, no. 5, pp. 2934–2951, 2021.

[12] A. Di Luzio, D. Francati, and G. Ateniese, "Arcula: A secure hierarchical deterministic wallet for multi-asset blockchains," in *Cryptology and Network Security: 19th International Conference, CANS 2020, Vienna, Austria, December 14–16, 2020, Proceedings 19*, Springer, 2020, pp. 323–343.

[13] C. Chuang, Ih. Hsu, and T. Lee, "A Two-Party Hierarchical Deterministic Wallets in Practice," *Cryptology ePrint Archive*, 2023.

[14] S. Alzahrani and T. U. Daim, "Analysis of the cryptocurrency adoption decision: Literature review," in *2019 Portland International Conference on Management of Engineering and Technology (PICMET)*, IEEE, 2019, pp. 1–11.

[15] K. S. Bennani and I. Arpaci, "Factors influencing individual and organizational adoption of cryptocurrencies," in *Cryptofinance: A New Currency for a New Economy*, World Scientific, 2022, pp. 147–169.

[16] P. Das, A. Erwig, S. Faust, J. Loss, and S. Riahi, "BIP32-Compatible Threshold Wallets," *Cryptology ePrint Archive*, 2023.

[17] J. Groth and V. Shoup, "On the security of ECDSA with additive key derivation and presignatures," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, 2022, pp. 365–396.

[18] Pieter Wuille, "BIP32 Proposal," https://github.com/bitcoin/bips/. Accessed: Feb. 20, 2024. [Online]. Available: https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki

[19] N. Ruggiano and T. E. Perry, "Conducting secondary analysis of qualitative data: Should we, can we, and how?," *Qualitative Social Work*, vol. 18, no. 1, pp. 81–97, 2019.

[20] Y. Xiao and M. Watson, "Guidance on conducting a systematic literature review," *J Plan Educ Res*, vol. 39, no. 1, pp. 93–112, 2019.

[21] J. Randolph, "A guide to writing the dissertation literature review," *Practical assessment, research, and evaluation*, vol. 14, no. 1, p. 13, 2019.

[22] M. Palatinus and P. Rusnak, "BIP44 Proposal," https://github.com/bitcoin/bips/blob/master/bip-0044.mediawiki. Accessed: May 10, 2024. [Online]. Available: https://github.com/bitcoin/bips/blob/master/bip-0044.mediawiki

[23] Chow Ava, "BIP174 Proposal." Accessed: May 12, 2024. [Online]. Available: https://github.com/bitcoin/bips/blob/master/bip-0174.mediawiki

[24] J. T. G. Swambo, "Evolving Bitcoin Custody," *arXiv preprint arXiv:2310.11911*, 2023.

[25] A. J. Cabrera-Gutiérrez, E. Castillo, A. Escobar-Molero, J. A. Álvarez-Bermejo, D. P. Morales, and L. Parrilla, "Integration of hardware security modules and permissioned blockchain in industrial iot networks," *IEEE Access*, vol. 10, pp. 114331–114345, 2022.