Blockchain Private Key Generation and Recovery

Subjects: Others

Contributor: Jungwon Seo, Deokyoon Ko, Suntae Kim, Vijayan Sugumaran, Sooyong Park, Jungwon Seo

As a future game-changer in various industries, cryptocurrency is attracting people's attention. Cryptocurrency is issued on blockchain and managed through a blockchain wallet application. The blockchain wallet manages user's digital assets and authenticates a blockchain user by checking the possession of a user's private key. Mnemonic codes are the most commonly used technique to generate and recover a private key in the blockchain wallet. Various studies have been conducted to improve the private key generation and recovery process.

Keywords: blockchain wallet ; blockchain ; blockchain private key

1. Introduction

Blockchain is expected to be applicable in various industries such as energy, health care, and finance [1][2][3][4][5][6][7]. As expected, various blockchain business models are appearing today, especially cryptocurrency business models which are currently attracting the attention of many. The first form of cryptocurrency started with Bitcoin and was initially not popular due to the malicious use of cryptocurrency [8], ICO (Initial Coin Offering) fraud [9][10], and volatility of values. However, recently, through DeFi (Decentralized Finance), CBDC (Central Bank Digital Currencies), and NFT (Non-Fungible Token), the value of cryptocurrency has been re-evaluated by interested individuals and entities. The interest in cryptocurrency can be observed through cryptocurrency exchanges such as CoinMarketCap [11]. In addition, various studies related to cryptocurrency are currently in progress [12][13][14][15][16][17].

In order to bring true changes beyond expectations, developers must not only overcome the technical limitations of blockchain; but also need to comprehensively analyze the blockchain wallet. The blockchain wallet is an application that bridges the gap between blockchain networks and the real world. The blockchain wallet helps a user access personal digital assets in blockchain networks. For example, a user can send cryptocurrency to others using a blockchain wallet. Moreover, the blockchain wallet authenticates a blockchain user by checking possession of a private key. The private key of the blockchain is an object that identifies the user without additional authentication from other institutions [18] and the private key can be generated and recovered through the blockchain wallet.

Mnemonic codes are the most commonly used technique to generate and recover a private key in the blockchain wallet. The mnemonic code technique used in blockchain uses the word list in BIP-0039 [19]. A private key is generated by combining 12 to 24 words out of 2048 words of the BIP-0039 list as a seed. Despite the widespread use of blockchain key generation and recovery using the mnemonic code technique, the technique is inefficient in private key generation and recovery. For example, when a user tries to generate a private key, they are faced with the inconvenience of finding a word list that can be used as a mnemonic code or the user needs to employ a mnemonic code generator on the Internet. Furthermore, if a user tries to recover a private key but cannot recall or locate the mnemonic code, recovery becomes impossible. A 2017 survey found that four-million Bitcoins were inaccessible due to the user's loss of a private key [20]. In addition, a company went bankrupt after it failed to recover its lost private key [21]. With these mentioned examples, accidents involving mnemonic code recovery failure continue to occur, suggesting that the mnemonic code technique does not consider usability in private key generation and recovery for users.

Various studies [22][23][24][25] to utilize a blockchain wallet are being conducted, as well as academic studies [26][27][28][29][30][31][32] to improve the current private key generation and recovery process. The most common studies [26][27][28][29] allowed other users or external repositories to participate in the process of generating and recovering a private key. These studies suggested storing core information for recovering a private key to external users or external repositories. These studies ensured private key recovery by storing core information to other users and external repositories during a private key generation process. However, there is a limitation that if external users or repositories with core information are attacked, there is a high risk that a private key is recovered by another user. In other studies [30][31], authors suggested using unique biometric information such as fingerprints to generate and recover private keys. In these studies, the safety and usability of generating and recovering a private key were ensured by using biometric information possessed only by the user.

However, there is the limitation of requiring special devices to collect biometric information. Another study [32] suggested that a user includes information for recovering a private key when generating the private key. In the study, the safety and usability of private key generation and recovery were ensured by utilizing information generated by a user. However, the results were limited in effectiveness as it did not improve significantly from the mnemonic code technique.

2. Blockchain and Cryptocurrency

Blockchain was started by fundamental academic studies from Stuart Haber [33], David Chaum [34], and Dave Bayer [35]. Blockchain is a data storage technology that allows all users to share and store all the data in the blockchain network. Because users share and store all data, the blockchain maintains the integrity and transparency of data. Data are validated by a consensus algorithm and they are stored in one block. Each block is connected back and forth and stored in the network, thus being called a blockchain. Blockchain technology consists largely of P2P (Peer-to-Peer) network, cryptography, and consensus algorithm.

Unlike the server–client network structure where servers are responsible for processing the broadcasting data and clients only read data and request to servers, in the P2P network each participating system acts as a server and client at the same time. The role of the P2P network in a blockchain ensures all participants can store data in a distributed manner. Furthermore, blockchain uses cryptographic techniques with a hashing algorithm and asymmetric key technology. By these cryptographic techniques, blockchain guarantees and verifies the integrity of data stored on a blockchain. Furthermore, a consensus algorithm ensures that all participants in a blockchain can store the same data. In a blockchain, cryptocurrency plays a role in inducing blockchain users to participate in a consensus algorithm. Blockchain users can acquire cryptocurrency as a reward to participate in a consensus algorithm or users can purchase cryptocurrency using traditional currency from cryptocurrency exchanges.

3. Blockchain Wallet and Cryptographic Key

An individual can use a blockchain wallet application after verifying ownership of the blockchain wallet by a simple mechanism such as a password. Furthermore, the blockchain wallet helps to connect a blockchain network by verifying possession of a private key from a blockchain user. Blockchain wallets can be classified as hot wallets and cold wallets. Hot wallets are a form of user's computer application or web extension program such as the Meta Mask [36]. Hot wallets have the advantage of being user-friendly because it is always connected to the Internet. However, there is a risk that cryptocurrency exploitation through network attacks can occur. Cold wallets refer to the storage of wallets on other physical devices separated from the user's computer such as a USB. Cold wallets can be secured from a hacker's network attack because it is separated from the user's computer, but has the disadvantage of being difficult to manage.

In cryptography, keys can typically be divided into symmetric-key algorithms that can be encrypted and decrypted with one key or asymmetric-key algorithms that require encryption and decryption to proceed with another key. Blockchain uses an asymmetric-key algorithm with ECDSA (Elliptic Curve Digital Signature Algorithm) [37] which consists of a private key and a public key. In a blockchain network, a private key is a unique random number that does not overlap with other users. It should be kept safe and not disclosed to others. A private key is used to encrypt transactions with other users. The public key can be disclosed to others and is used to decrypt transactions that are encrypted by a private key.

4. Research on Blockchain Private Key Generation and Recovery

Existing studies [26][27][28][29][30][31][32] on blockchain private key generation and recovery and these studies can be divided into three main categories.

- Studies that store core information related to a private key in other users' or external repositories at the time of the private key generation process and utilizes it for recovery [26][27][28][29].
- Studies to generate and recover a private key using user biometric information [30][31].
- A study that includes information for the recovery of a private key by users when they create private key [32].

Soltani and Nguyen et al. [26] suggested generating and recovering a private key by using KEP (Key Escrow Providers). In this study, KEP generates a main private key, and multiple sub-private keys and then provides them to a user. The main private key and sub-private keys have the same public key and the user mainly uses only the main private key. When the user loses the main private key, the user provides their assigned sub-private keys to KEP. The KEP recovers the main private key by applying the Lagrange Polynomial. Zhu and Chen et al. also proposed a study called HA-eWallet [27] which provides private key recovery information to an external repository. According their study, a user generates multiple private

keys at the time of the private key generation and stores all private keys in DRC (Disaster Recovery Center). Among the stored private keys, only one private key that has been user-selected is used primarily. During the private key recovery process, DRC recovers a lost private key to the user through ownership authentication for the other known keys then the lost ones.

He and Wu et al. [28] proposed an approach that combines specific seeds to generate a private key and transfers each seed to friends of a user in a blockchain network for enabling private key recovery. In this study, when a private key recovery is requested, the user's friends provide seeds to the user, and based on this, the user can recover the private key. Another study by He and Lin et al. [29] focused on private key generation and recovery using the DMCD (Dependent Multi-Constrained Derangement) and SKN (Shamir-Kademlia-Neighbor) methods. When a user generates a private key, they create additional private key fragments together. The user sends the fragments to other specific users who are selected by DMCD. During the private key recovery process, a user receives private key fragments from other users. The user verifies private key fragments by SKN and proceeds to recover the private key.

Another type of study utilizes biometric information from a user to generate and recover a private key. Aydard and Cetin et al. [30] utilized fingerprints to generate and recover a private key. To ensure the security of user biometric information, the researchers use the Reed–Solomon technique [38]. Zhao and Zhang et al. [31] proposed the use of BSN (Body Sensor Network) and Fuzzy Vault [39] techniques for generating and recovering a private key in the healthcare blockchain. In this study, a user utilizes IoT devices to build BSN to obtain user biometric information. When a user requests the recovery of a private key, the user can obtain their biometric information via BSN. After that, the user can recover the private key using the biometric information authenticated by Fuzzy Vault.

Signth and Stefanidis et al. [32] proposed PKRS (Partial Knowledge Recovery Scheme) for generating and recovering a user's private key. Their research proposal is similar to the mnemonic code technique used in traditional wallet applications. In wallet applications that use a mnemonic code technique, the user is required to remember multiple words to recover their private key, while Signth's study requires a user to remember answers to the user's own questions. When a user generates a private key, the user splits the private key to create private key fragments. Each of those private key fragments is created in a form that includes specific user-generated questions and answers. When a user requests private key recovery, they must answer questions that have been stored in private key fragments to activate and combine fragments to recover the private key.

References

1. 5 Blockchain Trends for 2020. Available online: https://www.fm-house.com/wp-content/uploads/2020/07/5-Blockchain-Trends-for-2020.pdf (accessed on 4 March 2022).
2. Chen, Y.; Lu, Y.; Bulysheva, L.; Kataev, M.Y. Applications of Blockchain in Industry 4.0:a Review. Inf. Syst. Front. 2022, 24, 1–15.
3. Zile, K.; Strazdina, R. Blockchain Use Cases and Their Feasibility. Appl. Comput. Syst. 2018, 23, 12–20.
4. Makridakis, S.; Christodoulou, K. Blockchain: Current Challenges and Future Prospects/Applications. Future Internet 2 019, 11, 258.
5. Burer, M.J.; de Lapparent, M.; Pallotta, V.; Capezzali, M.; Carpita, M. Use cases for Blockchain in the Energy Industry Opportunities of emerging business models and related risks. Comput. Ind. Eng. 2019, 137, 106002.
6. Le, T.; Hsu, C.; Chen, W. A Hybrid Blockchain-Based Log Management Scheme with Non-Repudiation for Smart Grids. IEEE Trans. Ind. Inform. 2021, 1–12.
7. Choi, T.; Siqin, T. Blockchain in logistics and production from Blockchain 1.0 to Blockchain 5.0: An intra-inter-organizati onal framework. Transp. Res. Part E 2022, 160, 102653.
8. Foley, S.; Karlsen, J.R.; Putnins, T.J. Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurr encies? Rev. Financ. Stud. 2019, 32, 1798–1853.
9. Trozze, A.; Kamps, J.; Akartuna, E.A.; Hetzel, F.J.; Kleinberg, B.; Davies, T.; Johnson, S.D. Cryptocurrencies and future financial crime. Crime Sci. 2022, 11, 1.
10. Hornuf, L.; Kuck, T.; Schwienbacher, A. Initial coin offerings, information disclosure, and fraud. Small Bus. Econ. 2022, 58, 1741–1759.
11. CoinMarketCap. Available online: https://coinmarketcap.com/ (accessed on 7 June 2022).

12. Lansky, J. Possible State Approaches to Cryptocurrencies. J. Syst. Integr. 2018, 9, 19–31.
13. Pelaez-Repiso, A.; Sanchez-Nunez, P.; Calvente, Y.G. Tax Regulation on Blockchain and Cryptocurrency: The Implications for Open Innovation. J. Open Innov. Technol. Mark. Complex. 2021, 7, 98.
14. Choi, T. Creating all-win by blockchain technology in supply chains: Impacts of agents' risk attitudes towards cryptocurrency. J. Oper. Res. Soc. 2021, 72, 2580–2595.
15. Mas'ud, M.Z.; Hassan, A.; Shah, W.M.; Abdul-Latip, S.F.; Ahmad, R. A Review of Digital Forensics Framework for Blockchain in Cryptocurrency Technology. In Proceedings of the 2021 3rd International Cyber Resilience Conference (CRC), Langkawi Island, Malaysia, 29–31 January 2021.
16. Liu, X.F.; Jiang, X.; Liu, S.; Tse, C.K. Knowledge Discovery in Cryptocurrency Transactions: A survey. IEEE Access 2021, 9, 37229–37254.
17. Varghese, H.M.; Nagoree, D.A.; Anshu; Jayapandian, N. Cryptocurrency Security and Privacy Issues: A Research Perspective. In Proceedings of the 2021 6th International Conference on Communication and Electronics Systems (ICCES); Coimbatre, India, 8–10 July 2021.
18. Li, X.; Jiang, P.; Chen, T.; Luo, X.; Wen, Q. A survey on the security of blockchain systems. Future Gener. Comput. Syst. 2020, 107, 841–853.
19. bitcoin/bips. Available online: https://github.com/bitcoin/bips/blob/master/bip-0039/english.txt (accessed on 5 February 2022).
20. Exclusive: Nearly 4 Million Bitcoins Lost Forever, New Study Says. Available online: https://fortune.com/2017/11/25/lost-bitcoins/ (accessed on 3 February 2022).
21. $190 Million in Crypto Gone Forever, How Canada's Biggest Bitcoin Exchange Lost it All. Available online: https://finance.yahoo.com/news/190-million-crypto-gone-forever-213010166.html (accessed on 3 February 2022).
22. Li, G.; You, L. A Consortium Blockchain Wallet Scheme Based on Dual-Threshold Key Sharing. Symmetry 2021, 13, 1444.
23. Gurfidan, R.; Ersoy, M. Blockchain-Based Music Wallet for Copyright Protection in Audio Files. J. Comput. Sci. Technol. 2021, 21, 11–19.
24. Han, J.; Song, M.; Eom, H.; Son, Y. An Efficient Multi-signature Wallet in Blokchain Using Bloom Filter. In Proceedings of the SAC'21: Proceedings of the 36th Annual ACM Symposium on Applied Computing, New York, NY, USA, 22–26 March 2021.
25. Sung, S. A new key protocol design for cryptocurrency wallet. ICT Express 2021, 7, 316–321.
26. Soltani, R.; Nguyen, U.T.; An, A. Practical Key Recovery Model for Self-Sovereign Identity Based Digital Wallets. In Proceedings of the 2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), Fukuoka, Japan, 4 November 2019.
27. Zhu, F.; Chen, W.; Wang, Y.; Lin, P.; Li, T.; Cao, X.; Yuan, L. Trust your wallet: A new online wallet architecture for Bitcoin. In Proceedings of the 2017 International Conference on Progress in Informatics and Computing (PIC), Nanjing, China, 15–17 December 2017.
28. He, S.; Wu, Q.; Luo, X.; Liang, Z.; Li, D.; Feng, H.; Zheng, H.; Li, Y. A Social-Network-Based Cryptocurrency Wallet-Management Scheme. IEEE Access 2018, 6, 7654–7663.
29. He, X.; Lin, J.; Li, K.; Chen, X. A Novel Cryptocurrency Wallet Management Scheme Based on Decentralized Multi-Constrained Derangement. IEEE Access 2019, 7, 185250–185263.
30. Private key encryption and recovery in blockchain. Available online: https://arxiv.org/abs/1907.04156 (accessed on 19 December 2020).
31. Zhao, H.; Zhang, Y.; Peng, Y.; Xu, R. Lightweight Backup and Efficient Recovery Scheme for Health Blockchain Keys. In Proceedings of the 2017 IEEE 13th International Symposium on Autonomous Decentralized System (ISADS), Bangkok, Thailand, 22–24 March 2017.
32. Singh, H.P.; Stefanidis, K.; Kirstein, F. A Private key Recovery Scheme Using Partial Knowledge. In Proceedings of the 2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Paris, France, 19–21 April 2021.
33. Haber, S.; Stornetta, W.S. How to time-stamp a digital document. J. Cryptol. 1991, 3, 99–111.
34. Chaum, D.; Fiat, A.; Naor, M. Untraceable Electronic Cash. CRYPTO 1988: Advances in Cryptology; Springer: New York, NY, USA, 1990.

35. Bayer, D.; Haber, S. Improving the Efficiency and Reliability of Digital Time-Stamping. In Sequences II Methods in Communication, Security, and Computer Science; Springer: New York, NY, USA, 1993.
36. Metamask. Available online: https://metamask.io/ (accessed on 8 June 2022).
37. Johnson, D.; Menezes, A.; Vanstone, S. The Elliptic Curve Digital Signature Algorithm (ECDSA). Int. J. Inf. Secur. 2001, 1, 36–63.
38. Reed, I.S.G. Solomon Polynomial codes over certain finite fields. J. Soc. Ind. Appl. Math. 1960, 8, 300–304.
39. Juels, A.; Sudan, M. A Fuzzy Vault Scheme. Des. Codes Cryptogr. 2006, 38, 237–257.