Jurnal Manajemen dan Teknologi Informasi (JMTI)
Volume 16, Issue 02, 2026, pp. 01-09
ISSN 2721-7604 (Online); ISSN 2087-5312 (Print)
DOI: 10.59819

PHONE-NUMBER-BASED IDENTITY ABSTRACTION FOR WEB3 WALLETS: A SYSTEMATIC LITERATURE REVIEW

Sarah Fajriah Rahmah[1)], **Annazma Ghazalba**[2]
[1]Syarif Hidayatullah State Islamic University Jakarta, Tangerang, Indonesia; *sarah.fajriah24@mhs.uinjkt.ac.id
[2]Independent Researcher, Bogor, Indonesia; anaznazma8@gmail.com
[1)]Corresponding author; sarah.fajriah24@mhs.uinjkt.ac.id

ARTICLE INFO
Article history
Received October 18, 2026
Revised October 20 , 2026
Accepted October 28, 2026
Available online October 31, 2026

Keywords: identity abstraction; Web3 wallet; phone number authentication; decentralized identity; systematic literature review

Copyright ©2026 by Author. Published by Faculty of Engineering and Informatics PGRI Mahadewa University Indonesia

Abstract. Web3 wallet adoption faces severe onboarding hurdles due to complex seed phrases and reliance on foreign social logins. Meanwhile, everyday transactions in emerging markets like Indonesia heavily rely on trusted phone number verification via SMS OTP. This study examines how this familiar habit can be leveraged as an identity abstraction method for Web3 wallets. Utilizing a Systematic Literature Review (SLR) under the PRISMA 2020 protocol, a search on Google Scholar via Publish or Perish yielded 156 initial records, narrowing down to 34 selected documents. The findings identify six primary research clusters: biometrics, social login, seed phrases, phone/SMS authentication, wallet usability, and decentralized identity theory. Crucially, existing literature shows that phone/SMS authentication remains strictly confined to conventional banking and e-government, never intersecting with Web3 wallet contexts. This separation highlights a significant research gap. The study concludes that utilizing phone numbers as an identity anchor for Web3 wallets in emerging markets presents a promising yet largely unexplored space, offering a localized, user-friendly alternative to mitigate adoption barriers.

INTRODUCTION

Storing a seed phrase remains one of the primary friction points for users interacting with a Web3 wallet for the first time. That 12- to 24-word recovery phrase serves as the absolute gateway to digital assets, offering no conventional recovery mechanism or forgot password option if misplaced (Jenis & Chandrasekar, 2026). While technical interventions—such as embedding phrases within digital images or applying Elliptic Curve Cryptography—improve data security, the fundamental burden of custody remains entirely on human discipline (Sentana et al., 2026).

To lower these adoption barriers, various identity abstraction mechanisms have emerged. Biometric authentication introduces fingerprint or facial recognition layers, though it relies heavily on device compatibility (Chauhan & Singh, 2022), and even a basic fingerprint-based access lock needs dedicated sensor hardware to be installed (Saputra et al., 2023). Alternatively, social login leverages Ethereum Account Abstraction (ERC-4337) standards to enable familiar credentials like Google or GitHub (Mavletova et al., 2026; Singh et al.,

2023). However, while social logins streamline onboarding, they reintroduce centralized dependencies that contradict the core ethos of decentralization.

In developing markets such as Indonesia, everyday financial and digital activities rely on a far more pervasive and trusted mechanism: the phone number. From opening bank accounts and using e-wallets like GoPay or OVO (Wardani et al., 2023) to executing e-commerce checkouts, SMS-based One-Time Passwords (OTP) form the bedrock of digital verification. Research on QRIS adoption among Indonesian street vendors likewise shows that transaction convenience motivates users, while limited technical knowledge and security concerns deter non-users (Armani & Sendjaja, 2025). Although extensive literature investigates SMS authentication protocols, implementation vulnerabilities, and applications in ATMs or e-government systems (Rahmon et al., 2026; Stęchły & Szpunar, 2023; Zhao et al., 2025), these studies remain strictly confined to conventional, reversible financial architectures. They fail to address how phone-number-based identity abstraction performs within trustless, irreversible Web3 environments.

This study bridges this gap by systematically mapping the landscape of Web3 wallet identity abstraction methods—spanning seed phrases, social logins, biometrics, and phone-number-based approaches—through a PRISMA 2020-compliant Systematic Literature Review. Given that emerging markets experience distinct technological trust dynamics (MSCI Inc., 2026), evaluating how phone numbers can serve as a secure identity anchor provides vital strategic insights for driving regional Web3 mass adoption.

RESEARCH METHODS

This study uses a Systematic Literature Review (SLR) approach following the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) 2020 protocol. The literature search was conducted on Google Scholar via the Publish or Perish (PoP) software using 13 keyword combinations (each limited to a maximum of two words): decentralized identity, biometric authentication, biometric wallet, social login, account abstraction, seed phrase, SMS authentication, phone identity, crypto wallet, wallet usability, wallet adoption, blockchain identity, and blockchain Indonesia.

A. Inclusion and Exclusion Criteria

The inclusion criteria comprised publications from 2022 to 2026; discussing identity, authentication, or identity abstraction methods related to wallets, blockchain, or Web3; written in Indonesian or English; and mostly sourced from peer-reviewed publications. Documents were excluded if they: only discussed conventional fintech e-wallets unrelated to blockchain (e.g., studies on GoPay or OVO adoption), discussed blockchain without touching on identity/wallet aspects, discussed biometrics outside a wallet/Web3 context, were mismatched search results caused by ambiguous keywords, or were commercial product pages and non-academic news.

B. Selection Process

The initial search yielded 156 records (identification). After removing 11 duplicates, 145 unique records remained and were screened by title and abstract, with 109 eliminated for not meeting the inclusion criteria. A total of 36 records advanced to the eligibility assessment stage, but 2 documents were subsequently excluded due to insufficient bibliographic data or unverifiable source credibility. The final result was 34 documents entering the analysis stage. The complete selection flow is illustrated in Figure 1.

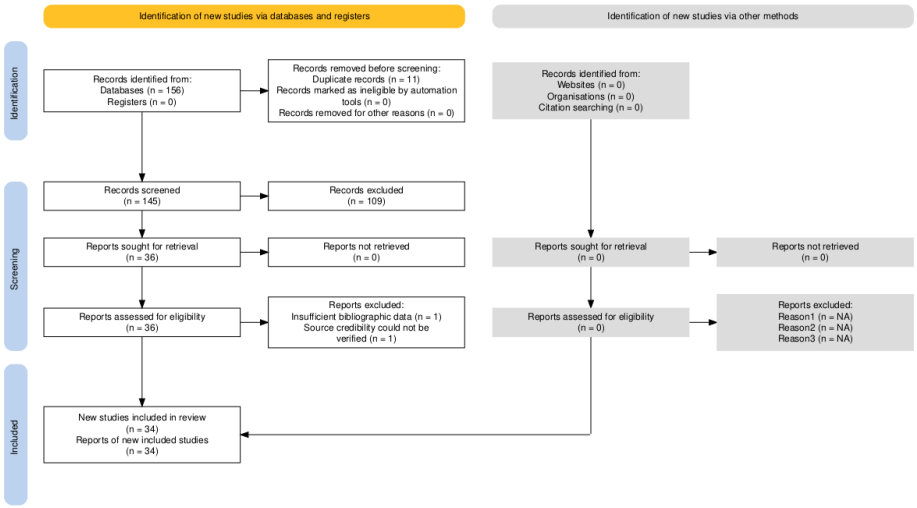


Figure 1: PRISMA Selection Flow Diagram

The 34 documents that passed selection were then grouped into six approach categories, as shown in Table 1. Sources cited outside these 34 documents (Armani & Sendjaja, 2025; Nikmat et al., 2024; Saputra et al., 2023; Wardani et al., 2023; MSCI Inc., 2026) were not part of the screened corpus and serve only as contextual support for the discussion.

Table 1. Distribution of Included Documentss by Approach Category

Approach Category	Count (n)	Percentage
Biometric-based	1	2.9%
Social login/account abstraction	2	5.9%
Seed phrase/traditional	2	5.9%
Phone/SMS-based	6	17.6%
Wallet usability	5	14.7%
General decentralized identity theory	18	52.9%
TOTAL	34	100%

RESULTS AND DISCUSSION

A. Existing Identity Abstraction Methods

In the biometric cluster, only one document was found, discussing a two-layer security mechanism for an IoT-based digital wallet using biometric data as an additional authentication factor (Chauhan & Singh, 2022). The social login/account abstraction cluster is represented by two documents: one on decentralized salary payment automation using the Ethereum Account Abstraction scheme (Mavletova et al., 2026), and another on the technical side of account abstraction through a singleton entrypoint contract and verifying paymaster on the Ethereum network (Singh et al., 2023).

The seed phrase cluster also contains only two documents, both concerned with cryptographically securing the storage of the recovery phrase—one through text-to-image encoding (Jenis & Chandrasekar, 2026), another through Elliptic Curve Cryptography in an Indonesian context (Sentana et al., 2026). Interestingly, neither touches on how ordinary users actually understand, or misunderstand, how seed phrases work; their focus is purely mathematical security, not user experience.

The phone number/SMS-based cluster has the most documents of all, six in total, but all of them revolve around conventional application domains: SMS authentication risk analysis (Stęchły & Szpunar, 2023), OTP implementation flaws (Zhao et al., 2025), two-factor

systems for ATMs (Rahmon et al., 2026), MD5 hash-based OTP security (Meiditra et al., 2025), two-layer authentication for e-government services (Abdullah, 2023), and a qualitative comparison of SMS/TOTP against FIDO2/WebAuthn and Passkeys from a practitioner's perspective (Folorunsho & Odeleye, 2025). Not one of these six documents discusses its application specifically within a Web3 wallet.

Looking more closely, the content of these six documents is fairly diverse. The qualitative comparison study found that although SMS and TOTP are considered more affordable and easier for ordinary users to understand than FIDO2/WebAuthn or Passkeys, practitioners also judge both as more prone to operational disruption (Folorunsho & Odeleye, 2025). Meanwhile, risk assessment and implementation flaws studies highlight SMS's vulnerability to interception and manipulation at both the network and device level (Stęchły & Szpunar, 2023; Zhao et al., 2025). This pattern is consistent with what occurs in ATM and e-government authentication systems: SMS OTP remains widely used for its convenience, even though its vulnerabilities have long been known and documented (Abdullah, 2023; Rahmon et al., 2026).

The wallet usability cluster contributes five documents highlighting various challenges in using Web3 wallets in general: UX pattern analysis on mobile crypto wallets (Plaquin et al., 2024), Web3 wallet security and privacy (Wang & Van Cutsem, 2024), usability evaluation of the Bitcoin Lightning wallet (Leder, 2024), strengthening security and usability through post-quantum cryptography and zero-knowledge proof (Kethepalli et al., 2023), and designing a crypto wallet more accessible for blind users (Zhou et al., 2023).

The general decentralized identity theory cluster is by far the largest, with 18 documents covering a wide range of technical focuses. Several documents build self-sovereign frameworks on smart contracts with provably secure privacy schemes (Beesabathuni, 2026; Zhang & Wang, 2026), while others contribute conceptual, security, and bibliometric studies on blockchain-based digital identity (Khaund, 2025; Judijanto, 2025; Monaghan, 2026). A number of documents propose zero-knowledge proof and range proof schemes specifically for selective disclosure (Ramya et al., 2025; Zhu et al., 2023), and one integrates AI with Merkle trees for identity verification (Le et al., 2025).

On the cross-sector application side, this study found decentralized identity applied to education for verifying academic credentials (Jain, 2025), to cross-border digital services for simplifying identity verification across jurisdictions (Dubey et al., 2025), and—most relevant to the Indonesian context—to Know Your Customer (KYC) processes in the banking industry (Irwanto et al., 2023). In addition, three patent documents were found, indicating industry interest in this topic: a QR-code-based decentralized identity method (Vivek et al., 2026), an anti-fraud system for SMS OTP authentication (Rule et al., 2025), and a trust/user identity model for distributed systems (Naqvi et al., 2022). Rounding out this cluster are a study on blockchain implementation algorithms for decentralized identity authentication systems (Xie, 2024), a design science approach investigating DID technology (Krupicka, 2024), a review on blockchain identity management (Bamnote & Patil, 2023), and a prototype for a blockchain-based national identity storage security system in Indonesia (Fathiyana et al., 2022).

B. Trust, Security, and Ease of Use

These four methods are essentially answering the same question—who is trusted to safeguard a user's identity—but with mutually opposing answers, and each answer carries concrete consequences.

With seed phrases, trust rests entirely with the user, with no intermediary whatsoever. The consequence is immediate: once the phrase is lost or forgotten, no party—neither the wallet developer nor an exchange—can recover it, because that is simply how private-key cryptography works. Improvement efforts so far, such as encoding the phrase into a digital image (Jenis & Chandrasekar, 2026) or wrapping it with Elliptic Curve Cryptography (Sentana et al., 2026), only address how to store the phrase more safely, not how to reduce the risk of a user forgetting or mis-copying it in the first place.

Social login takes the exact opposite path: trust is shifted to a third-party identity provider such as Google or GitHub (Mavletova et al., 2026; Singh et al., 2023). As a result, users do not need to remember anything, but the wallet's security becomes only as strong as the security of that third-party account itself. If the Google account is hacked or phished, the Web3 wallet linked to it is put at risk too, contradicting Web3's decentralized philosophy.

Biometrics sit somewhere in between: a fingerprint or face cannot be "forgotten," but once that data is leaked, a user cannot simply swap it out the way they would change a password (Chauhan & Singh, 2022). This method also requires owning a device with an adequate sensor, as fingerprint-based access systems depend on dedicated sensor hardware (Saputra et al., 2023)—something not evenly available to everyone, particularly outside major cities.

Table 2. Comparison of Security Trade-Offs and Ease of Use Across Methods

Method	Who Is Trusted	Consequence of Failure	Burden on the User
Seed phrase	Entirely with the user	If lost, it's gone - no reset option	Heavy - requires strict self-custody discipline
Social login/AA	Shifted to Google/GitHub, etc.	As secure as that third-party account	Light - just log in as usual
Biometric	Tied to the user's body	Biological data cannot be replaced if leaked	Moderate - requires supporting hardware
Phone number/SMS	Dependent on mobile carrier	Vulnerable to SIM swap and SMS interception	Light - already an everyday habit

Phone numbers occupy a unique position compared to the other three methods. Their security trade-off—vulnerability to SIM swap and SMS interception—is nothing new; this is precisely the risk conventional banking has faced for decades, and mitigations already exist for it: transaction anomaly detection, real-time notifications, and daily transaction limits. What differs in a Web3 context is that the consequence of a mitigation failure is far more severe: blockchain transactions are final and cannot be reversed, unlike bank transactions. This means adopting phone numbers as an identity anchor for Web3 wallets requires additional mitigation layers specifically designed for the irreversible nature of blockchain transactions—something not yet widely addressed in conventional SMS OTP literature (Abdullah, 2023; Rahmon et al., 2026; Stęchły & Szpunar, 2023). Structured IT risk-management approaches already applied to Indonesian information systems, such as ISO 31000 (Nikmat et al., 2024), could serve as a starting point for designing these layers.

From this it is clear that no single method wins outright. What sets phone numbers apart is that they impose the lightest burden on users among methods whose security can still be

relied upon—something particularly relevant in Indonesia, where transaction convenience is a main driver of QRIS use among street vendors (Armani & Sendjaja, 2025) and phone number penetration is far more even than biometric devices or Google/GitHub accounts. This does not mean phone numbers are automatically ready to deploy; rather, the gap in mitigating transaction-finality risk is precisely the homework that needs solving.

C. How Far This Research Has Reached Southeast Asia, Particularly Indonesia

Of the 34 documents analyzed, only 3 (8.8%) explicitly address a Southeast Asian context, particularly Indonesia: seed phrase security on cryptocurrency wallets using ECC (Sentana et al., 2026), SMS-based OTP security systems for general information systems (Meiditra et al., 2025), and decentralized identity for banking KYC processes (Irwanto et al., 2023). None of these three documents discuss phone numbers as an identity abstraction method used specifically for Web3 wallets. This shows that the intersection between local financial infrastructure and Web3 wallets remains very rarely examined academically.

D. The Unexplored Space

Drawing this together, research on SMS/phone number authentication is well established in conventional domains (Rahmon et al., 2026; Stęchły & Szpunar, 2023; Zhao et al., 2025), and research on decentralized identity and Web3 wallets has also grown considerably. Yet both run along separate tracks, never intersecting. Not a single document in this review specifically synthesizes phone numbers as an identity abstraction method for Web3 wallets—even though, in developing countries like Indonesia, phone numbers are trusted and evenly owned. This reflects a structural mismatch: SMS/OTP studies originate from telecommunications security focusing on reversible transactions, whereas decentralized identity studies stem from blockchain engineering evaluating trustless, irreversible models. Neither community has systematically explored what happens when a trust anchor built for reversible transactions is applied to a context where transactions cannot be reversed at all.

CONCLUSION

This systematic review of 34 documents reveals a distinct divide between conventional SMS authentication research and Web3 wallet identity solutions. While methods such as seed phrases, social logins, and biometrics offer varying trade-offs between security and ease of use, phone numbers present a uniquely accessible identity anchor, particularly for emerging markets like Indonesia. However, this approach remains largely unexplored in Web3 contexts. Because blockchain transactions are irreversible, utilizing phone numbers requires robust mitigation layers against established risks, such as SIM swapping, that go beyond conventional banking standards. To bridge this gap, future research should move beyond conceptual discussions and prioritize empirical testing of phone-based Web3 wallets, such as the Saku prototype, to evaluate Social Identity Abstraction in real-world scenarios. Expanding literature databases beyond Google Scholar and conducting direct usability and security evaluations will be critical in refining this identity model for wider adoption.

REFERENCES

Abdullah, S. M. (2023). A two-layer authentication security through personal mobile SMS for KRG-Iraq e-government system. Eurasian Journal of Science and Engineering.

Armani, D. P. I., & Sendjaja, T. (2025). Analisis keputusan adopsi teknologi QRIS pada pedagang kaki lima: Perspektif pengguna dan non-pengguna. Jurnal Manajemen dan Teknologi Informasi, 15(2), 115–124. https://doi.org/10.59819/jmti.v15i2.5382

Bamnote, A., & Patil, R. Y. (2023). Identity management using blockchain - A review. International Journal of Darshan Institute on Engineering Research and Emerging Technologies (IJDI-ERET), 12(1), 29–35.

Beesabathuni, H. N. (2026). Decentralized identity management via blockchain-based smart contracts: A cryptographic self-sovereign framework. International Journal of Intelligent Systems and Data Science.

Chauhan, T., & Singh, A. (2022). Two-layered security mechanism for enhanced biometric security of IoT based digital wallet. In S. Goundar, A. Purwar, & A. Singh (Eds.), Applications of artificial intelligence, big data and internet of things in sustainable development (Chapter 14). CRC Press/Routledge.

Dubey, A. K., Kesharwani, K., Shubneet, Yadav, A. R., Talwandi, N. S., & Polam, R. M. (2025). Decentralized identity management using blockchain for secure cross-border digital services. 2nd International Conference on Advanced Computing and Emerging Technologies (ACET), Ghaziabad, India.

Fathiyana, R. Z., Yutia, S. N., & Hidayat, D. J. (2022). Prototype of integrated national identity storage security system in Indonesia using blockchain technology. JOIV: International Journal on Informatics Visualization, 6(1).

Folorunsho, F., & Odeleye, Z. (2025). Comparing multi-factor authentication methods from SMS and TOTP to FIDO2/WebAuthn and Passkeys: A qualitative study of practitioner perspectives. GlobeIS International Journal of Global Information Systems.

Irwanto, F., Jodis, J., Indrakusuma, E., & Gui, A. (2023). Decentralized identity (DID) for Know Your Customer (KYC) process in the banking industry. IEEE 9th International Conference on Computing, Engineering and Design (ICCED). https://doi.org/10.1109/ICCED60214.2023.10425153

Jain, A. (2025). Blockchain-based decentralized identity systems in education. Scientific Journal of Artificial Intelligence and Blockchain Technologies (SJAIBT), 2(4), 30–38. https://doi.org/10.63345/sjaibt.v2.i4.104

Jenis, M. R. A., Chandrasekar, A., Ramachandran, H., & Dhinnesh, A. D. C. N. (2026). A secure octal-based text-to-image encoding scheme for seed phrase encryption and decryption. World Conference on Computational Science and Technology (WcCST), 904–909.

Judijanto, L. (2025). Mapping blockchain identity management research: A bibliometric analysis (2010-2025). The Eastasouth Journal of Information System and Computer Science, 3(2), 202–213. https://doi.org/10.58812/esiscs.v3i02.862

Kethepalli, Y., Joseph, R., Vajrala, S. R., Vemula, J., & Naik, N. S. (2023). Reinforcing security and usability of crypto-wallet with post-quantum cryptography and zero-knowledge proof. arXiv preprint. https://doi.org/arXiv:2308.07309

Khaund, B. (2025). Decentralized identity using blockchain: Enhancing security and privacy in digital identity management. Journal of Computer Science and Technology Studies, 7(6), 858–866. https://doi.org/10.32996/jcsts.2025.7.6

Krupicka, J. (2024). A design science approach to investigating decentralized identity technology. Cybersecurity Undergraduate Research Showcase, William & Mary.

Le, H. V. A., Nguyen, Q. D. N., Tadashi, N., & Tran, T. H. (2025). Blockchain-based decentralized identity management system with AI and Merkle trees. Computers (MDPI), 14(7), Article 289. https://doi.org/10.3390/computers14070289

Leder, M. (2024). Design, implementation and usability evaluation of the AfriBit Bitcoin Lightning Wallet (Bachelor's thesis). Department of Informatics, Universitat Zurich.

Mavletova, K., Madhwal, Y., & Yanovich, Y. (2026). Decentralized salary payment automation using Ethereum account abstraction. In R. Li (Ed.), Blockchain technology and applications (pp. 384–395). Springer Nature Switzerland.

MSCI Inc. (2026). MSCI annual market classification review 2026. June 2026.
Meiditra, I., Candra, D. G. A., Rahmansyah, R., Yuda, F., & Selvanda, A. R. (2025). Design and development of information system security with authentication using one-time password identification based on SMS with MD5 Hash. Internet of Things and Artificial Intelligence Journal, 5(2), 444–461. https://doi.org/10.31763/iota.v5i2.926
Monaghan, J. (2026). Blockchain, digital identity, and self-sovereign identity. In E. Tan (Ed.), Handbook of blockchain in public governance (pp. 195–205). Edward Elgar Publishing. https://doi.org/10.4337/9781035330096.00026
Naqvi, S. A., Raucci, R. F., & Puppala, G. (2022). User identity and trust models in decentralized and distributed systems. U.S. Patent No. 11,496,313.
Nikmat, A., Apriyadi, M. F., Kahfi, M. A., & Aibi, O. N. (2024). Analisis manajemen risiko teknologi informasi pada sistem informasi akademik (SIAK) Universitas Muhammadiyah Sukabumi (UMM) menggunakan ISO 31000. Jurnal Manajemen dan Teknologi Informasi, 14(1), 49–58. https://doi.org/10.59819/jmti.v14i1.3321
Plaquin, L., Gindre, F., & Urbieta, M. M. (2024). Mobile crypto wallet user experience patterns analysis. XIV Jornadas de Cloud Computing, Big Data y Emerging Topics, La Plata, Argentina.
Rahmon, H. A., Adavize, A. A., Jimoh, T. G., Dan, E. E., & Esang, M. O. (2026). Development of a two-factor authentication system for ATMs using SMS one-time passwords. Proceedings of the ASUP Maiden International Conference, Federal Polytechnic, Ukana Chapter, 778.
Ramya, M., Anuvarshini, B. S., Kanika, G., Lohith, A., & Barath, B. (2025). Enhancing decentralized identity management with zero-knowledge proofs for selective disclosure. 6th International Conference on Electronics and Sustainable Communication Systems (ICESC), Coimbatore, India. https://doi.org/10.1109/ICESC65114.2025.11212333
Rule, J., Douglas, L., & Macomber, J. (2025). Systems and methods of reducing fraud for sms otp authentication. U.S. Patent App. 18/223,617. Google Patents.
Saputra, I. W. A. E., Arta, I. K. J., & Ambaradewi, N. L. G. (2023). Rancang bangun sistem keamanan pintu laboratorium komputer dengan fingerprint berbasis mikrokontroler (Arduino Uno). Jurnal Manajemen dan Teknologi Informasi, 13(2), 57–64. https://doi.org/10.59819/jmti.v13i2.3087
Sentana, I. K. A., Putra, I. G. N. A. C., Putri, L. A. A. R., & Rahayuda, I. G. S. (2026). Keamanan seed phrase dalam wallet cryptocurrency menggunakan algoritma Elliptic Curve Cryptography (ECC). Jurnal Elektronik Ilmu Komputer Udayana (JELIKU), 15(1), 99–104.
Singh, A. K., Hassan, I. U., Kaur, G., Kumar, S., & Anmol (2023). Account abstraction via singleton entrypoint contract and verifying paymaster. 2nd International Conference on Edge Computing and Applications (ICECAA). https://doi.org/10.1109/ICECAA58104.2023.10212316
Stęchły, A., & Szpunar, A. (2023). Analysis of potential risks of SMS-based authentication. Advances in Web Development Journal, 1(1). https://doi.org/10.5281/zenodo.10049987
Vivek, V., LeFebre, E., & Dunstan, S. (2026). Decentralized identity methods and systems. U.S. Patent No. 12,614,193. State Farm Mutual Automobile Insurance Company.
Wang, W., & Van Cutsem, T. (2024). Poster: I know what crypto you got last summer: A study on Web3 wallet security and privacy. 6th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), 1–2.
Wardani, N. W., Nirwana, N. K. A., Ratnaningrum, L. P. R. A., & Salimah, S. H. (2023). Analisis kualitas layanan dan pengguna aplikasi OVO terhadap kepuasan pelanggan

menggunakan PIECES framework. Jurnal Manajemen dan Teknologi Informasi, 13(2), 123–132. https://doi.org/10.59819/jmti.v13i2.3205

Xie, Y. (2024). Research on blockchain implementation algorithm for decentralized identity authentication system. IEEE Conference Publication.

Zhang, Y., & Wang, Z. (2026). Formalizing privacy in decentralized identity: A provably secure framework with minimal disclosure. IACR ePrint Archive (Preprint). https://doi.org/eprint.iacr.org/2026/077

Zhao, J., He, F., Yang, Y., & Zhang, Y. (2025). Identifying implementation flaws of SMS OTP authentication. IEEE Transactions on Mobile Computing, 24(9), 7899–7913. https://doi.org/10.1109/TMC.2025.3550883

Zhou, Z., Sharma, T., Emano, L., Das, S., & Wang, Y. (2023). Iterative design of an accessible crypto wallet for blind users. Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023), 381–398. USENIX Association.

Zhu, X., He, D., Bao, Z., Luo, M., & Peng, C. (2023). An efficient decentralized identity management system based on range proof for social networks. IEEE Open Journal of the Computer Society, 4, 84–96. https://doi.org/10.1109/OJCS.2023.3258188