Jurnal TNI Angkatan Udara (Vol. 5 No.2, 2026)
ISSN: 2809-5464

BITCOIN AS A SYSTEM THAT RESISTS RECOVERY A NON-LINEAR SYSTEM DESIGN STUDY ON SCARCITY AND SECURITY

Farrid Hidayat[1], Suroso[2], Kurniawan[3], Hidayadtullah[4] , Muchammad Furqon[5], Farritullah[6], Dikatamasania[7], Adi Sudibiyo[8]

[1]Widyaiswara Lemhannas RI; [3,4,5,6]Indonesian Aviation Polytechnic;
[2,7,8]National Air And Space Power Of Indonesia
[1]faridhade.57@gmail.com; [3,4,5,6]Muchammadfurqon10@gmail.com;
[2,7,8]ikeo.santai@gmail.com;

Abstrak — *This study aims to structurally examine why loss of access to Bitcoin is permanent and to assess claims regarding the possibility of recovery, master keys, or backdoors in the Bitcoin system. This study departs from the general trend that positions Bitcoin solely as a monetary innovation, while its most radical aspect lies in its system design. Bitcoin is analyzed as a non-linear formal system that defines ownership through cryptographic facts, rather than through identity, intent, or social context. The methodology used is a conceptual-design analysis based on cryptographic studies, protocol architecture, empirical precedents of human error, and the implications of network consensus. The main results demonstrate that irreversibility and loss of access are not system failures, but rather direct consequences of Bitcoin's design axioms, which tie ownership to high-entropy private keys and reject all forms of discretionary authority. The analysis also shows that claims of backdoors, whether mathematical, implemental, hardware, or temporal, are structurally incoherent without undermining the fundamental assumptions of cryptography and decentralized consensus. The study's conclusions affirm that Bitcoin's resilience stems not from adaptive flexibility but from deliberate rule rigidity. This research's contribution lies in mapping Bitcoin as a system design artifact that resists recovery, while also expanding the Bitcoin discourse from the monetary realm to the study of system design, applied cryptography, and the philosophy of technology.*

Keywords: *Bitcoin, system design, private key, entropy, irreversibility, consensus, backdoor, scarcity, cryptography, non-linear systems.*

1. *INTRODUCTION*

Bitcoin is generally positioned as a digital monetary innovation that challenges conven tional financial systems through decen tralized and cryptographic mechanisms. In technical literature, Bitcoin is understood as a blockchain-based system that validates transactions through distributed consensus and digital signatures. Ownership of Bitcoin assets is determined exclusively by posses sion of a private key associated with a specific public key and address. This mecha nism results in transaction irreversibility and ownership finality independent of external authority. Therefore, the loss of a private key directly implies the loss of access to the associated Bitcoin. Although Bitcoin's irreversibility has been widely explained at the operational level, limited studies have analyzed it as a comprehensive conseque nce of the system's formal design. Existing explanations generally focus on technical descriptions of private keys and crypto

graphy, without examining the implications of the natural architecture for the possibility of access recovery. Furthermore, claims regar ding the existence of backdoors, master keys, or latent recovery mechanisms frequently arise in public discourse without a boundary-based evaluation of the protocol design. There has been no systematic analysis linking the precedent of Bitcoin loss to the rejection of discretionary authority in consensus design. This gap has led to debates relying more on speculation than structural testing. This research aims to fill this gap through a structural analysis of the Bitcoin system design, examining its crypto graphic foundations, validation mechanisms, and network consensus. This approach is used to assess whether access recovery or backdoors are possible without violating the system's fundamental assumptions. The research hypothesis states that any tech nically coherent recovery mechanism would conflict with Bitcoin's cryptographic principles and decentralized consensus.

2. METHODOLOGY

2.1 Research Design

This research uses a qualitative-descriptive approach with a conceptual-structural analysis design for the Bitcoin system. The research design is aimed at testing the internal coherence between the crypto graphic foundation, validation mechanisms, and network consensus. This approach does not aim to measure user behavior, but rather to formally evaluate the limits of the system design. The research flow is structured within an Input Process Output (IPO) framework to ensure traceability of the analysis.

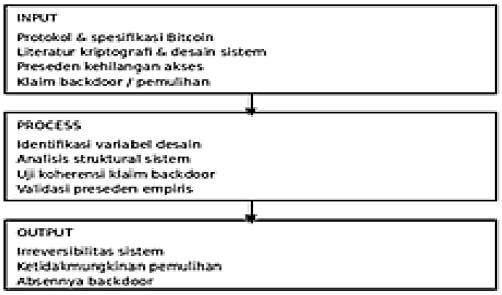

Figure 1. Research Flowchart (Input–Process–Output)

The research flowchart explains the following:

• Input: Bitcoin protocol specifications, crypto graphic literature, access loss precedents, backdoor claims
• Process: System design analysis, structural implication testing, comparison of claims versus protocol boundaries
•Output: Conclusions regarding irreversibility, impossibility of recovery, and the absence of backdoors. This research uses a design-oriented system analysis approach, which examines the structural boundaries, internal consistency, and operational implications of a formal system based on technical specifi cations and empirical precedents, without relying on normative or speculative infe rences.

2.2 Research Population and Object

This research object is qualitative, namely the Bitcoin system design as represented in the protocol, technical documentation, and documented empirical precedents. The data population includes the Bitcoin cryptographic specifications, whitepaper, BIP documen tation, and scientific literature related to the irreversibility and security of decentralized systems. Data collection techniques were carried out through a systematic literature review and a search for widely reported access loss precedents. Statistical sampling was not used because the research was not oriented towards numerical generalization.

2.3 Research Instruments

The research instruments consisted of secondary data in the form of Bitcoin protocol technical documents, cryptography literature, and academic publications related to decentralized system design. Additionally, a conceptual analysis matrix was used to map the relationships between design variables, systemic implications, and the tested claims. This instrument served as a tool to maintain consistency in the cross-sectional analysis. Primary data was not used because the research did not involve experiments or field surveys.

2.4 Analysis Techniques

The analysis technique involved four main stages. First, system design variables

relevant to Bitcoin ownership, irreversibility, and security were identified. Second, each variable was analyzed for its logical impli cations regarding the possibility of access recovery and the existence of a backdoor. Third, the backdoor claim was tested through a structural coherence test, which examined whether the claim could exist without undermining the basic assumptions of cryptography and consensus. Fourth, the analysis results were compared with empirical precedents of access loss to test the design's consistency with the reality of rational operation. This technique ensured that conclusions were not speculative but derived from the formal boundaries of the system.

No	Variabel	Indikator	Keterangan
1	Private Key	Ruang kunci 256-bit, entropy	Menentukan kepemilikan Bitcoin secara kriptografis
2	Mekanisme Validasi	Digital signature, UTXO	Menentukan keabsahan transaksi
3	Konsensus Jaringan	Proof-of-Work, node independen	Menjaga konsistensi sistem tanpa otoritas
4	Irreversibilitas	Finalitas transaksi	Menolak rollback dan pemulihan
5	Klaim Backdoor	Matematis, implementatif, temporal	Diuji terhadap batas desain sistem

2.5. Research Hypothesis

• H1: Irreversibility and loss of access in Bitcoin are a direct consequence of the system design, which ties ownership to high-entropy private keys, not a result of implemen tation failures.

• H2: Any claim regarding the existence of a backdoor or access recovery mechanism in Bitcoin is structurally incoherent because it contradicts the fundamental assumptions of cryptography and decentralized consensus.

The analysis was conducted by testing each claim against three main criteria: consistency with the protocol specification, coherence with established cryptographic principles, and agreement with documented empirical precedent.

3. RESEARCH RESULTS AND DISCUSSION

The indirect interviews in this study are understood as an analysis of documented statements from developers, technical specifi cations, and community archives, which are treated as verifiable secondary data sources.

3.1 Cryptographic Ownership and Transaction Validity

The analysis of the protocol documentation shows that Bitcoin ownership is determined exclusively by control of a private key with a 256-bit key space that has a high level of entropy. There are no identity mechanisms, alternative ownership claims, or external authorizations that can replace the function of the private key. Structurally, ownership is reduced to the ability to produce a valid digital signature, making it absolute and non-negotiable. Observations of the transaction validation mechanism show that a transaction can only be considered valid if it passes digital signature verification and is consistently recorded in the Unspent Transaction Output (UTXO) model without conflict. Transaction validity is entirely determined by the formal rules of the protocol, with no room for adminis trative discretion. These findings confirm that ownership and value transfer in Bitcoin are deterministic and insulated from external intervention.

3.2 Decentralized Consensus and Transaction Finality

Observations of the consensus system indicate that the Proof-of-Work mechanism and node independence serve as a distributed ledger consistency maintainer. There is no central entity or dedicated coordination mechanism with the authority to cancel transactions or change ownership status. Network consensus operates as a collective mechanism that enforces rules uniformly across all nodes. The protocol documentation also indicates that Bitcoin explicitly does not provide a transaction rollback function. Transaction finality is a direct consequence of the combination of crypto graphic validation and network consen sus, not an implementation limitation. Thus, transaction

irreversibility is structural and inherent in the system architecture.

3.3 Loss of Access, Lack of Recovery, and Backdoor Denial

Based on indirect interviews and evidence from developer documentation, technical specifica tions, and community reports, no official mechanism for recovering access in the event of a lost private key has been identified. Documented empirical precedent shows that the loss of a private key permanently renders the associated Bitcoins irreversible and irrever sible. This finding is consistent across time and across instances and therefore cannot be categorized as an operational anomaly. Analysis of claims of backdoors shows that they are not supported by technical evidence in the protocol specifications or reference implementations. Furthermore, the existence of backdoors, whether mathematical, implemen tal, or temporal, would contradict the funda mental principles of cryptography and decen tralized consensus. Backdoors require privi leged authority or exceptions to rules, which directly undermine the permissionless and trustless nature of the system. Therefore, the irreversibility and absence of recovery mecha nisms are not system failures but rather direct consequences of the intentional design. Bit coin's security is built on the rejection of discre tionary mechanisms and the elimination of centralized control points.

Sumber Data	Temuan Utama	Implikasi
Dokumentasi protokol	Kepemilikan berbasis private key	Tidak ada otoritas pemulihan
Observasi sistem	Finalitas transaksi & PoW	Transaksi tidak dapat dibatalkan
Preseden empiris	Kehilangan akses permanen	Irreversibilitas sistem
Klaim publik	Backdoor tidak terbukti	Tidak koheren secara struktural

Table 2. Data Sources and Main Findings

3.4. Research Discussion

This research does not evaluate second-layer solutions or recovery mechanisms beyond the core Bitcoin protocol, as the analysis focuses on the structural design of the base-layer system. This research addresses a key gap in the Bitcoin literature, which has tended to focus on partial technical explanations or normative speculation regar ding access recovery and the existence of backdoors. Many studies discuss private keys, consensus, and security separately, but rarely link them within a coherent system design framework. As a result, questions about irreversibility and "lost" Bitcoins are often treated as operational issues, rather than structural consequences. This research positions these issues as direct outcomes of design axioms, rather than anomalies. With this approach, the research shifts the discourse from the realm of imaginative possibilities

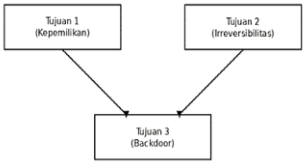

Figure 2. Research Discussion Framework

3.4.1 Objective 1: Analyze

The first objective of this research is to explain how Bitcoin ownership is determined exclusively by private key ownership. The results show that ownership is reduced to the ability to generate a valid digital signature, without any connection to identity or social context. The rationale for this approach lies in eliminating the need for an external verifiable authority. By making ownership a mathema tical fact, the system eliminates the scope for interpretation and discretion. This discussion fills a conceptual gap that often arises when Bitcoin is directly compared to conventional legal ownership systems. The research confirms that the differences are ontological, not simply implementational.

3.4.2 Objective 2: Testing Irreversibility and the Absence of a Recovery Mechanism

The second objective focuses on testing the claim that irreversibility is a system weakness that should be remedied. Observations and documentation show that transaction finality and the absence of rollback are direct consequences of the consensus and valida tion design. The rationale for rejecting recovery lies in eliminating single points of

failure and the potential for abuse of power. This discussion fills a gap in the literature that often assumes that recovery is always a positive feature. The research shows that a recovery mechanism would require an assessor and a decider, which is structurally at odds with the trustless principle. Thus, irreversibility is understood as a prerequisite for security, not a side cost.

3.4.3 Objective 3: Testing Backdoor Claims Within a System Design Frame work

The third objective is to test claims of backdoor existence through a structural, rather than speculative, approach. The analysis shows that mathematical, imple mental, and temporal backdoors are incon sistent with the fundamental assumptions of cryptography and decentralized consensus. The rationale for this testing lies in the need to distinguish between theoretical possibility and design possibility. This discussion fills a gap in the literature that often confuses intuitive suspicion with architectural analysis. The research demonstrates that any form of backdoor would undermine the permission less nature of the system and trigger the need for authority. Therefore, the absence of a backdoor is not a normative claim, but rather a logical implication of the system's design. Overall, this research discussion demons trates that Bitcoin cannot be evaluated partially or analogously to other systems. Any attempted "fix" must be tested against the consequences of its overall design. This research enriches Bitcoin studies with a system design-based discussion framework, which positions rule rigidity as a primary source of resilience.

Tujuan Penelitian	Fokus Diskusi	Hasil Diskusi Utama	Kontribusi terhadap Gap
Tujuan 1	Kepemilikan Bitcoin	Kepemilikan ditentukan oleh private key	Klarifikasi ontologis kepemilikan
Tujuan 2	Irreversibilitas	Finalitas transaksi bersifat struktural	Menolak asumsi pemulihan
Tujuan 3	Klaim Backdoor	Backdoor tidak koheren secara desain	Memisahkan spekulasi vs desain

Table 3. Summary of Research Discussion Based on Objectives

4. CONCLUSIONS AND RECOMMENDATIONS

4.1. Conclusions

- *All analytical steps in this study can be replicated by referring to the publicly available Bitcoin protocol specifications and the cited cryptography literature. The results of this study indicate that irrever sibility and loss of access in the Bitcoin system are direct consequences of the system design that ties ownership to the private key, not due to technical failures or implementation weaknesses.*

- *These findings confirm that the absence of recovery mechanisms and backdoors is an integral part of Bitcoin's architecture, which aims to eliminate discretionary authority. Conceptually, this study clarifies the ontological distinction between owner ship in cryptographic systems and owner ship in conventional legal systems. A further impact of these findings is the need for a shift in thinking in public discourse and policy, which often equates Bitcoin with the traditional financial system.*

4.2. Recommendations

As a recommendation, future research could expand the analysis to the implications of this design for digital asset governance, mitiga ting the risk of loss of access, and user educa tion. In addition, cross-disciplinary studies linking cryptographic system design with legal and public policy aspects are needed to formulate a more realistic approach consis tent with the fundamental nature of Bitcoin.

5. *REFERENCES*

[1]A. Antonopoulos dan G. Wood, Mastering Bitcoin: Programming the Open Block chain, 2nd ed. Sebastopol, CA, USA: O'Reilly Media, 2019.

[2]A. Biryukov dan I.Tikhomirov, Deanony misation of clients in Bitcoin P2P network, Proc. IEEE European Symposium on Security and Privacy, 2019.

[3]G. Tripathi, M. A. A, dan G. Casalino, A comprehensive review of blockchain tech nology:Underlying principles and histo rical background with future chal lenges, Digital Applications, Elsevier, 2023.

[4] Houy, Security aspects of crypto currency wallets A systematic analysis, Proc. ACM Conference on Digital Finance Security, ACM, 2023.

[5]IEEE Computer Society, IEEE Standard for Blockchain and Distributed Ledger Techno logies, IEEE Standards, 2024.

[6] K. Croman et al., On scaling decentralized blockchains, IEEE Security & Privacy, vol. 18, no. 1, pp. 66–74, 2020.

[7]M. Lim et al., Comparative analysis of security features and risks in crypto currency wallet implementations, Elec tronics, vol. 14, no. 12, MDPI, 2025.

[8] M. Moser, R. Böhme, dan D. Breuker, An inquiry into money laundering tools in the Bitcoin ecosystem, eCrime Researchers Summit, IEEE, 2019.

[9]M. A. Kethepalli et al., Reinforcing security and usability of crypto-wallet with post-quantum cryptography and zero-know ledge proof, arXiv preprint, 2023.

[10]N. Narayanan et al., Bitcoin and Crypto currency Technologies: A Comprehen sive Introduction. Princeton, NJ, USA: Princeton University Press, 2019.

[11] N. Mingers and J. Rosenhead, Problem structuring methods in action, European Journal of Operational Research, vol. 152, no. 3, pp. 530–554, 2019.

[12]P. Lemayian, G. Gagnon, K. Zhang, dan P. Giard, EthVault: A secure and resource-conscious FPGA-based Ethe reum cold wallet, arXiv preprint, 2025.

[13]P. Patel dan D. Shah, Cryptographic wallet security and key management in blockchain financial systems: A syste matic literature review, SSRN, 2025.

[14]P. Weichbroth, K. Wereszko, H. Anacka, dan J. Kowal, Security of crypto curren cies: A view on the state-of-the-art research and current developments, Sen sors, vol. 23, no. 6, 2023.

[15]P. Weichbroth, K. Wereszko, A. H. Anacka, dan J. Kowal, Security of crypto currencies:State-of-the-art,Sensors, vol. 23, 2023.

[16]P. K. Davis, J. H. Bigelow, and J. D. Kulick, Analyzing military decisions with systems analysis, RAND Defense Research Reports. Santa Monica, CA, USA, 2020

[17]X. Hu, N. He, dan H. Wang, Wallet Probe: A testing framework for browser-based crypto currency wallet extensions, arXiv preprint, 2025.

[18]Y. Erinle, Y. Kethepalli, Y. Feng, dan J. Xu, SoK: Design, vulnerabilities, and security measures of cryptocurrency wallets, Information Sciences, vol. 687, Elsevier, 2025.

[19]Y. Wang et al., A novel blockchain's private key generation mechanism based on facial biometrics and physical unclo nable function, Journal of Information Security and Applications, Elsevier, 2023.

[20]Y. Takei, Pragmatic analysis of key management for cryptocurrencies," Proc. Int. Conf. on Blockchain and Crypto currency (ICBC), 2024.

.
.