Social Development Studies, 2026, Volume 2, Issue 3
https://www.bbwpublisher.com/journal/SDS
Online ISSN: 3083-3868
Print ISSN: 3083-3876

Minimum Viable Decentralisation for Blockchain-Enabled Philanthropy: A Governance Framework for Verifiable Accountability under Intensive Regulatory Oversight

Yan Lin

Zhejiang University, Hangzhou 310000, Zhejiang, China

Copyright: © 2026 Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), permitting distribution and reproduction in any medium, provided the original work is cited.

Abstract: This article develops Minimum Viable Decentralisation (MVD) for blockchain-enabled philanthropy under intensive regulatory oversight. MVD shifts attention from node counts to verification rights: statutory authority and organisational liability may remain centralised, but one effective controller should not dominate key evidence, claim validation, material rule changes, and external review. Five non-compensatory conditions are specified: source independence, independent validation authority, constrained material rule changes, portable external review, and accountable intervention with remedies. A closure test, removal-to-failure test, and risk tiering operationalise the framework. MVD does not measure social impact; it asks whether material operational claims are independently reviewable. Blockchain is warranted only where it adds verifiable accountability beyond credible databases and independent audit.

Keywords: Blockchain-enabled philanthropy; Minimum viable decentralisation; Decentralisation of verification rights; Verifiable accountability; Permissioned blockchain governance; Intensive regulatory oversight

Online publication: June 30, 2026

1. Introduction: From “blockchain transparency” to “who controls verification?”

Transparency is not the same as factual verifiability. Non-profit transparency research distinguishes accessibility, completeness, and accuracy [1]Managed-transparency research shows that organisational actors may still control visibility [2]. The issue here is who controls the evidence and permissions needed for verification. Blockchain can protect records but cannot prove off-chain performance or replace beneficiary voice and organisational accountability [3]. The question is therefore who can independently verify material claims. Blockchain philanthropy now includes permissioned chains, audit, regulatory embedding, and

multi-tier validation. ClearGive combines these features [4]Multiple nodes or regulatory participation alone therefore do not establish meaningful decentralization. This article asks which verification-related rights must be separated when regulatory authority remains centralised. MVD refers to decentralisation of verification rights, not dispersal of administrative authority or organisational liability.

2. Literature review and theoretical positioning

2.1. Charity regulation: From transparency to verifiable accountability

Disclosure concerns what is made public; record-integrity verification concerns whether records were signed or altered; substantive verification concerns whether payments, delivery, or services occurred. Verifiable accountability requires authorised external actors to access relevant evidence, review inconsistencies, and use workable correction or challenge procedures. Immutability therefore cannot be treated as proof of off-chain truth.

2.2. Blockchain philanthropy: From traceability architectures to regulatory compatibility

Existing work already provides traceability, permissioned-chain, and audit components. The further issue is whether actors hold independent evidence, keys, and practical refusal rights, or merely repeat signatures under common control. Evaluation therefore concerns the allocation of verification rights, not the number of system modules.

2.3. Decentralisation: From network property to allocation of governance rights

Blockchain governance research treats decentralisation as an allocation of decision rights and accountability rather than a purely technical property [5]. Reviews locate centralisation across network, consensus, operational, and governance layers [6]. DAO research has framed sufficient decentralisation as a verifiable condition [7]. This article narrows the problem to philanthropic evidence chains: public authority may remain centralised, but critical verification rights should not form a single-controller loop.

2.4. Off-chain facts, the Oracle problem, and technology adoption boundaries

Philanthropic projects depend on off-chain facts and thus face the oracle problem: external inputs reintroduce trusted sources and single points of failure [8]. Bank receipts, logistics records, and invoices each prove only limited propositions. Legal responsibility also constrains technical dispersal; charity-law research still requires identifiable fiduciary responsibility [9]. If a trusted database and independent audit already cover material risks, blockchain may add little [10].

Table 1. Related research and the analytical gap

Research stream	Established contribution	Question addressed here
Transparency	Disclosure and perceived transparency	Who controls verification?
Blockchain philanthropy	Permissioned chains and audit	Are nodes genuinely independent?
Governance	Decentralisation as allocation of authority	Which rights must be separated?
Off-chain facts	External inputs and technological alternatives	When does blockchain add value?

The gap is the absence of a clear standard for how much separation of control is sufficient for

independent review.

3. Research design and institutional boundaries

3.1. Materials, unit of analysis, and mechanism-based reasoning

This conceptual study integrates research on non-profit transparency, blockchain philanthropy, blockchain governance, and the oracle problem with Chinese charity and digital-platform rules. The unit of analysis is a material operational claim, such as receipt of funds, disbursement, delivery, service completion, or a permission change. MVD evaluates evidence provenance and reviewability, not distributive fairness or overall social impact. The single-controller closure test asks whether one controller can dominate evidence production, claim validation, material rule changes, and review. The removal-to-failure test asks whether that control loop reappears when an independent safeguard is removed.

3.2. Chinese institutional context: Centralised authority and dispersed verification rights

Chinese internet fundraising is regulated through rules on eligibility, platforms, payment, and disclosure. The Charity Law assigns disclosure and financial responsibilities to charitable organisations[11]The 2026 platform measures specify verification and information duties while separating platform services from payment settlement[12]; and the Personal Information Protection Law requires purpose limitation, data minimisation, and protection of sensitive information[13]. MVD separates regulatory authority from verification rights rather than replacing legal responsibility with node consensus. China is the framework's institutional setting, not a universal template. Cross-jurisdictional use requires remapping responsibility, evidence, data protection, and intervention powers.

4. Minimum viable decentralisation: Concept, necessary conditions, and operationalisation

4.1. Definition and boundary

MVD is the minimum separation of verification-related control required, under relevant legal duties and risks, to prevent one actor from controlling material claims, validation, material rule changes, and external review. "Minimum" denotes indispensable safeguards, "viable" sufficient review and correction capacity, and "decentralisation" verification-related control rather than public authority generally. MVD addresses verifiable accountability only; it does not replace beneficiary participation, internal governance, professional evaluation, or social-impact assessment.

4.2. Five non-compensatory minimum conditions

The five conditions are non-compensatory: no single condition, such as node numbers, public dashboards, or an auditor, can offset common evidence inputs, shared key custody, or review wholly dependent on one platform.

Table 2. MVD: Five necessary conditions, checks, and failure modes

Dimension	Minimum condition	Check	Failure mode
1. Evidence source	External or cross-source evidence	Producer and shared inputs	Executor controls all evidence
2. Validation authority	Executor is not the sole final validator	Keys, access, appointment	One party holds multiple keys

Dimension	Minimum condition	Check	Failure mode
3. Rule change	Validity rules require cross-party authorization	Eligibility, thresholds, recovery	One party lowers the threshold
4. External review	Evidence remains independently reviewable	Export and outage tests	Verification fails outside platform
5. Intervention accountability	Privileged acts are justified and reviewable	Restricted logs where needed	Unlogged change or obstruction of lawful action

4.3. Effective control, material rule change, and closure tests

Effective control covers technical, informational, and organisational control plus material economic dependence. Shared infrastructure alone is insufficient; actors should be treated as one controller where one party can sign for several parties, reset permissions, monopolise evidence, or deprive validators of a practical refusal right. The closure test asks whether one controller can select evidence, validate claims, alter validity rules, and impede external review. If removing a safeguard recreates this loop, the safeguard is necessary. Multiple nodes may still amount to a single control where one provider holds operational and validation keys, replaces validators, and disables evidence export.

5. Regulatory-compatible implementation: Risk tiering, evidentiary conflict, and privacy constraints

5.1. Risk tiering: Retaining all five functions while adjusting intensity

Verification intensity may vary by value, irreversibility, beneficiary sensitivity, dispute likelihood, and the difficulty of verifying off-chain facts. Higher-risk projects require more heterogeneous evidence, stronger independent review, and tighter authorisation. Risk tiering changes verification intensity, not the presence of the five governance functions.

Table 3. Risk-tiered implementation of MVD

Risk	Features	Verification	Cost/privacy
Low	Low value/reversible	Batch records; sampled review	Existing database tools
Medium	Contracts/services	Independent evidence	Sensitive data off-chain
High	High value/irreversible/sensitive	Second-level review; multi-party authorisation	Selective disclosure

5.2. Off-chain evidentiary conflict: From majority signatures to tiered dispute handling

Multiple evidence sources should expose inconsistency rather than let majority signatures decide off-chain truth. Systems should preserve pending, partially verified, and unverifiable states and route disputes to reviewers outside the operator's control. A second source or regulatory investigation is warranted where collusion or material consequences are suspected. Subjective social outcomes should not be reduced to binary on-chain claims.

5.3. Statutory intervention, confidentiality exceptions, and third-party review

Auditability of regulatory intervention does not require immediate public disclosure. Confidential matters may use restricted logs, sealed records, or delayed disclosure while preserving authorised review. Conformity review should examine key custody, authority over material rules, evidence export, and verification

continuity if the platform becomes unavailable.

5.4. Privacy protection: From data transparency to proof availability

Sensitive beneficiary data should normally remain off-chain, with only necessary states or proofs recorded on-chain. Privacy techniques can reduce disclosure but do not remove responsibility for verifying underlying facts.

6. Propositions and blockchain adoption criterion

Five propositions follow: independent evidence should improve conflict detection; effective control should explain review resilience better than node counts; portability should constrain platform-controlled presentation; separation of regulatory and verification rights should improve ex post explainability; and blockchain should be adopted only where governance gains exceed added costs. **Table 4** lists indicators. Blockchain may outperform conventional databases only where several organisations must maintain a shared state, no single operator is sufficiently trusted, and verification continuity after exit has practical value.

Table 4. Propositions, judgements, and observable indicators

Proposition	Judgement	Indicator
P1 Evidence	Independence improves conflict detection	Support/conflict rates
P2 Control	Effective control explains review resilience	Independent keys/unilateral rights
P3 Portability	Off-platform review limits selective presentation	Export and outage verification
P4 Layering	Layered authority improves explainability	Authorisation matching
P5 Net gain	Benefits should exceed verification costs	Cost and continuity

7. Cross-jurisdictional portability: Transferring conditions, not templates

MVD does not export a Chinese technical model. Its portable question is institutional: which powers must remain concentrated and accountable, and which verification rights would undermine independent review if commonly controlled? Without identifiable responsibility, independent review, or basic remedies, technical separation cannot substitute for legal accountability. Comparison should ask what rights must be separated for the same verification risk under different responsibility regimes.

Table 5. Institutional mapping before cross-jurisdictional application of MVD

Institutional dimension	Question to establish	Implication for MVD
Organisational/fiduciary liability	Who bears final responsibility?	Identify non-delegable authority
Fundraising access	Is licensing or a designated platform required?	Set identity and publication rights
Payment custody	Who may settle donations?	Link to lawful payment rails
Audit evidence	Who is qualified to verify?	Define validators
Data protection	How are sensitive data treated?	Set disclosure boundaries
Intervention and remedy	How can measures be reviewed?	Define privileged operations

8. Theoretical contributions, practical implications, and limitations

8.1. Theoretical contributions

First, MVD shifts decentralisation from node counts to verification rights and effective control. Second, transparency becomes reviewable accountability only when evidence and review procedures are not under the information provider's unilateral control. Third, regulatory compatibility is treated as layered authority: enforcement and organisational liability may remain centralised, while factual verification, material rule changes, and external review should not be unnecessarily concentrated.

8.2. Practical implications

MVD is first a test of whether blockchain is warranted. Evaluation should compare credible database alternatives and examine effective control, key custody, rule changes, evidence export, and continuity after platform failure. "Multiple nodes" or "immutability" do not by themselves establish independent verification.

8.3. Limitations and future testing

This is a conceptual study. The five conditions require testing through audits, simulations, and comparative cases; thresholds for effective control and risk also need empirical calibration, especially where economic dependence, outsourcing, or collusion is possible. MVD covers only part of accountability, and cross-jurisdictional portability remains untested.

9. Conclusion

The central question for blockchain philanthropy is whether technology changes control over factual verification, not whether a permissioned chain is used or how many nodes exist. MVD permits centralised regulatory authority while requiring that key evidence, claim validation, material rule changes, and external review do not all remain under one effective controller.

If a conventional database and independent audit can provide equivalent verification and correction at lower cost, blockchain should not receive priority. MVD identifies when separation of verification rights can add governance value.

Disclosure statement

The author declares no conflict of interest.

References

[1] Dethier F, Delcourt C, Dessart L, 2024, Donor Perceptions of Nonprofit Organizations' Transparency: Conceptualization and Operationalization. Nonprofit and Voluntary Sector Quarterly, 53(5): 1230–1260.

[2] Zhang Y, 2026, Managed Transparency as Platform-Era Decoupling in Internet Philanthropy: Evidence from China. Business & Society, 0: 0.

[3] Kuruppu S, Dissanayake D, de Villiers C, 2022, How Can NGO Accountability Practices Be Improved With Technologies Such as Blockchain and Triple-Entry Accounting? Accounting, Auditing & Accountability Journal, 35(7): 1714–1742.

[4] Roy GM, Ali SA, Aakash, Sharma C, Kumar A, Vijay R, 2026, ClearGive: A Governance-Driven Blockchain

Framework for Enhancing Transparency, Auditability, and Regulatory Compliance in Digital Philanthropy. EDPACS, 1–10.

[5] Beck R, Müller-Bloch C, King JL, 2018, Governance in the Blockchain Economy: A Framework and Research Agenda. Journal of the Association for Information Systems, 19(10): 1020–1034.

[6] Sai AR, Buckley J, Fitzgerald B, Le Gear A, 2021, Taxonomy of Centralization in Public Blockchain Systems: A Systematic Literature Review. Information Processing & Management, 58(4): 102584.

[7] Axelsen H, Jensen JR, Ross O, 2022, When Is a DAO Decentralized? Complex Systems Informatics and Modeling Quarterly, 31: 51–75.

[8] Caldarelli G, 2020, Understanding the Blockchain Oracle Problem: A Call for Action. Information, 11(11): 509.

[9] Shillito MR, 2026, Decentralised Governance and the Fiduciary Architecture of Charity Law: The Limits of DAO Integration. Information & Communications Technology Law, 1–24.

[10] Wüst K, Gervais A, 2018, Do You Need a Blockchain? 2018 Crypto Valley Conference on Blockchain Technology, 45–54.

[11] Standing Committee of the National People's Congress, 2023, Charity Law of the People's Republic of China (2023 Amendment).

[12] Ministry of Civil Affairs, Ministry of Industry and Information Technology, Cyberspace Administration of China, 2026, Measures for the Administration of Internet Public Fundraising Service Platforms, visited on March 22, 2026, http://big5.www.gov.cn/gate/big5/www.gov.cn/gongbao/2026/issue_12866/202607/content_7075898.html

[13] Standing Committee of the National People's Congress, 2021, Personal Information Protection Law of the People's Republic of China.

Publisher's note

Bio-Byword Scientific Publishing remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.