Fact Funders: A Transparent, Decentralized Crowdfunding Platform on Algorand

Greeshma G[1], Dhanush K[2], Keerthi R[3], Bharathi M[4]

[1,2,3,4] *Dept. of Computer Science and Engineering (Data Science), Vardhaman College of Engineering, Hyderabad, India*

---***---

Abstract - *Crowdfunding has become a vital channel for financing creative projects, startups, and social causes. Despite its popularity, existing centralized crowdfunding platforms suffer from fundamental limitations, including lack of transparency, risks of fund mismanagement, and little accountability from project creators once funds are disbursed. This paper introduces Fact Funders, a decentralized crowdfunding platform implemented on the Algorand blockchain that addresses these challenges by combining milestone-based funding releases, community-driven governance, and automated refund mechanisms. The system ensures that funds are only disbursed incrementally after verifiable project progress, validated through weighted donor voting. Contributions are safeguarded by smart contracts which act as controlled escrow accounts, while inactivity triggers refunds to protect donor interests. We detail the architecture, contract logic, and governance model, followed by an experimental deployment on Algorand TestNet. Results indicate that Fact Funders enhances transparency, reduces risk of fraud, and builds donor trust without compromising scalability or efficiency. This work demonstrates how blockchain-enabled governance can reshape crowdfunding ecosystems and provides a foundation for more accountable decentralized finance applications.*

Key Words: Blockchain, Algorand, Smart Contracts, Decentralized Applications, Crowdfunding, Governance, Milestone-based Funding, Escrow Mechanisms

1. INTRODUCTION

The rise of crowd funding platforms such as Kick starter, Indiegogo, and GoFundMe has enabled millions of individuals and organizations to raise funds directly from communities. By bypassing traditional financial intermediaries, crowd funding has democratized access to capital for startups, artistic endeavors, and charitable causes. However, despite its success, trust and accountability remain significant challenges.

In traditional platforms, creators often receive the entire fund pool once a campaign reaches its target. This lump-sum disbursement creates multiple risks:

- **Moral Hazard:** Creators may misuse funds without fulfilling promises.
- **Abandonment Risk:** Projects can be abandoned after receiving funds, leaving donors powerless.
- **Transparency Deficit:** Donors have limited visibility into project progress or fund usage.
- **Platform Dependency:** Centralized platforms act as gatekeepers, charging high fees and controlling dispute resolution.

Blockchain technology presents a promising alternative. Its inherent immutability, decentralization, and programmability through smart contracts can eliminate intermediaries, enforce accountability, and automate fund flows. In this paper, we introduce Fact Funders, a decentralized crowdfunding system built on the Algorand blockchain.

Fact Funders addresses the above shortcomings by:

- dividing projects into milestones, each with specific deliverables and funding amounts;
- releasing funds incrementally, only upon donor approval of milestone completion;
- incorporating community governance, where donors vote on progress validation with weighted influence proportional to their contributions;
- ensuring security and fairness via escrow, inactivity-triggered refunds, and Sybil-resistance mechanisms.

Contributions: This work makes the following key contributions:

- A milestone-based decentralized crowdfunding architecture on Algorand with escrow-protected fund custody.
- A square-root weighted governance model that balances donor influence while mitigating plutocratic dominance.
- An inactivity-triggered refund mechanism that protects donors against project abandonment.
- A functional prototype with smart contract deployment and frontend integration validated on Algorand TestNet.

2. RELATED WORK

The evolution of crowdfunding has been shaped by both centralized platforms and decentralized alternatives. Early crowdfunding systems, such as Kickstarter and Indiegogo, offered global visibility and reduced entry barriers, but their centralized structure created issues of accountability, transparency, and trust. Researchers have consistently highlighted risks such as lack of enforceable accountability once funds are disbursed, information asymmetry, and excessive reliance on platform operators.

The introduction of programmable blockchains enabled smart contracts and decentralized applications, forming a foundation for trust-minimized crowdfunding platforms. Studies have examined how blockchain can improve transparency and traceability in domains such as finance and healthcare, emphasizing the importance of decentralization, auditability, and privacy preservation [1], [11], [20].

In healthcare and other sensitive domains, blockchain has been adopted to improve data access control, audit trails, and consent management [2], [6], [10]. Similar principles can be applied to crowdfunding where stakeholder trust and verifiable records of actions are crucial. Reviews of blockchain research point out that while decentralization offers security and transparency benefits, open systems must carefully address scalability, privacy, and governance challenges [3], [11].

For crowdfunding specifically, milestone-based and escrow-driven models have been proposed, where smart contracts hold funds and only release them upon verifiable progress or approval by backers. Governance mechanisms including token-weighted voting and reputation systems have also been explored to address concentration of power and accountability. Fact Funders builds upon these ideas by integrating milestone-based escrow, square-root weighted donor governance, and inactivity-triggered refunds in a single Algorand-based platform.

3. PROPOSED APPROACH

The Fact Funders platform is designed to address three major deficiencies identified in both traditional crowdfunding and earlier blockchain-based implementations:

1) Lack of accountability in fund disbursement,
2) Concentration of power in centralized authorities or wealthy stakeholders, and
3) Absence of robust protection mechanisms for donors in cases of project abandonment.

To overcome these challenges, the proposed approach integrates milestone-based escrow management, square-root weighted donor governance, and inactivity-triggered refunds, all implemented within an Algorand ARC4 smart contract. This section elaborates on the system architecture, smart contract design, governance mechanisms, operational workflow, and security considerations of Fact Funders.

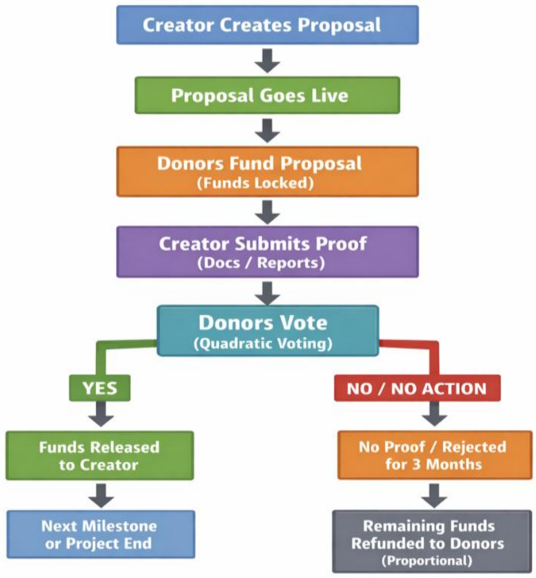

Fig -1: Architecture of the Fact Funders Decentralized Crowdfunding Platform

3.1 System Architecture

The architecture of Fact Funders consists of three primary entities and one governing protocol layer:

Project Creators – Individuals or organizations initiating crowdfunding campaigns. Creators specify project metadata (title, description, category, total funding goal) and subdivide the total funding requirement into up to five distinct milestones. Each milestone includes a descriptive label, funding amount, and expected deliverables.

Donors – Community members who contribute Algorand tokens (Algos) to projects. Donors not only provide financial support but also serve as governance participants, voting on milestone completion and fund release.

Algorand Smart Contract (ProposalContract) – The core protocol layer that governs fund custody, milestone approvals, disbursement, and refunds. It ensures compliance with predefined rules and executes transactions autonomously without intermediaries.

External Infrastructure – Optional off-chain resources such as GitHub repositories, decentralized storage (e.g., IPFS), or content delivery networks used by creators to submit proof of milestone completion. While off-chain data is external, links are stored on-chain for transparency.

3.2 Smart Contract Design

The Fact Funders smart contract is written in Python using the AlgoPy ARC4 framework and compiled for deployment on Algorand. Its design builds on the literature of milestone-based crowdfunding contracts, but incorporates governance and refund mechanisms absent in many earlier works. The contract exposes six primary methods, each mapped to an abimethod in ARC4:

- **create_proposal:** Initializes new campaigns with validation rules (e.g., sum of milestones must equal total funding goal, at least one milestone required, maximum of five milestones allowed).
- **donate_proposal:** Records donor contributions, enforces escrow by holding funds within the contract, and updates donor statistics.
- **submit_proof:** Enables creators to submit evidence of milestone completion, sets the voting window (48 hours), and resets vote tallies.
- **vote_milestone:** Allows donors to vote, applying square-root weighted voting to compute influence.
- **claim_milestone:** Releases milestone funds to creators if votes in favor exceed votes against after the voting period ends.
- **refund_if_inactive:** Allows donors to reclaim proportional contributions if the project remains inactive beyond 3 months (approximately 7,776,000 seconds).

3.3 Governance Model

Governance is central to Fact Funders' accountability mechanism. The platform employs a square-root weighted voting system.

1) Rationale for Square-Root Voting: Fairness small donors retain meaningful influence, addressing critiques of purely plutocratic one-token-one-vote systems. Proportionality larger donors contribute more financially and thus deserve greater, but not unlimited, influence. Sybil Resistance weighting by donation value, combined with square-root scaling, makes it prohibitively expensive to create multiple identities with small donations to manipulate outcomes.

2) Voting Workflow: Eligibility only donors who contributed at least 1 Algo are eligible to vote, preventing trivial spam. Weight Calculation if donor i contributes di Algos, their voting weight is $\sqrt{di}$. Decision Rule a milestone is approved if the sum of votes in favor exceeds the sum of votes against after the voting period. Time Constraint voting closes after 48 hours, ensuring timely resolution and fund flow.

3.4 Security Considerations

The Fact Funders platform incorporates multiple safeguards to mitigate common risks in decentralized crowdfunding systems.

- **Sybil Attacks:** Square-root weighted voting reduces incentives for identity splitting by limiting linear voting amplification.
- **Fund Misuse:** Smart contract escrow ensures that funds are only released upon milestone approval.
- **Collusion Risk:** Distributed donor voting mitigates centralized manipulation, although coordinated voting remains a potential governance challenge.
- **Inactivity Protection:** The refund mechanism protects donors against abandoned projects by enabling proportional withdrawals after prolonged inactivity.
- **Proof Integrity:** While milestone proofs are submitted off-chain, on-chain references maintain transparency and auditability.

4. EXPERIMENTAL SETUP

The purpose of the experimental evaluation is to validate the functionality, performance, and robustness of the Fact Funders platform under realistic crowdfunding conditions. Since crowdfunding involves diverse actors, financial transactions, and governance dynamics, the experimental setup was designed to emulate end-to-end workflows of project creation, donation, milestone validation, voting, fund disbursement, and refund triggering. This section provides a detailed account of the deployment environment, experimental scenarios, test cases, metrics, and monitoring methods used to evaluate the system.

4.1 Environment Configuration

Blockchain Network:

All experiments were conducted on the Algorand TestNet, chosen because it replicates mainnet conditions while using test tokens (Algos) to avoid real-world financial risks. TestNet provides realistic transaction latencies, block confirmation times, and fee structures, making it suitable for prototyping and evaluation.

Smart Contract Compilation and Deployment:

The ProposalContract was implemented in Python using the AlgoPy ARC4 framework. The contract was compiled and deployed using Algokit, an Algorand development and deployment toolkit. Deployment was configured to append applications on updates and preserve state across iterations. A minimum balance of 1 Algo was transferred to the contract's escrow account at creation to satisfy Algorand's application requirements.

Hardware and Software Environment:

- **Development Machine:** Ubuntu 22.04 LTS, 16 GB RAM, Intel i7 CPU.
- **Algorand Node:** TestNet access via Algorand Sandbox.
- **Programming Languages:** Python 3.10 (AlgoPy, Algokit), JavaScript (frontend simulation).
- **Monitoring Tools:** Python logging, Algorand Explorer (blockchain transaction monitoring), and Algokit utilities for debugging.

4.2 Operational Workflow

The lifecycle of a crowdfunding campaign in Fact Funders proceeds in six phases:

1) **Proposal Creation:** The creator defines project details and milestones. Contract validation ensures milestones sum correctly to the total funding goal.
2) **Fundraising:** Donors contribute via the donate_proposal function. Contributions are recorded, and donors gain governance rights proportional to their contribution.
3) **Proof Submission:** Upon completing a milestone, the creator submits a proof link. This triggers the governance process.
4) **Voting Phase:** Donors cast weighted votes within a 48-hour window. All votes are recorded transparently on-chain.
5) **Fund Disbursement:** If approvals exceed rejections, the milestone's funds are released to the creator via an internal payment transaction. Otherwise, funds remain in escrow until further progress is demonstrated.
6) **Refunds:** If no proof is submitted within 3 months, donors may invoke refund if inactive to reclaim proportional contributions.

4.3 Experimental Results Overview

- **Transaction Costs:** Average transaction costs per function call remained below 0.001 Algo. This validates Algorand's suitability for micro-donation scenarios, unlike some networks where high fees make small contributions impractical.
- **Latency:** Transaction confirmation times averaged between 4–6 seconds, consistent with Algorand TestNet expectations. This ensures timely campaign updates, critical for maintaining donor engagement.
- **Functional Correctness:** All validation rules executed correctly. For example, attempts to create proposals with milestones not summing to the total goal failed with appropriate error messages. Donors who attempted to vote without contributions were rejected.
- **Governance Simulation:** The square-root weighted scheme performed as designed: a donor contributing 7 Algos held approximately 2.65 vote weight versus a donor with 1 Algo (weight 1). This reduced absolute dominance while respecting financial input. In test scenarios, minority donors retained meaningful influence.
- **Refund Execution:** Refunds executed proportionally. For instance, in a 10-Algo raised project where 5 Algos remained unused, a donor contributing 2 Algos received exactly 1 Algo back.

5. RESULTS AND DISCUSSION

Figures 2 and 3 illustrate the implemented user interface of the Fact Funders platform. The landing page provides project discovery and navigation features, while the fundraiser creation interface enables creators to configure milestone-based funding requirements with validation ensuring consistency between total goals and milestone allocations. The experimental setup described in the previous section was executed across a series of test scenarios to assess the performance, correctness, and robustness of the Fact Funders platform. The results confirm that the system achieves its primary objectives of enhancing accountability, ensuring fair governance, and protecting donor contributions while maintaining scalability and cost-efficiency on the Algorand blockchain.

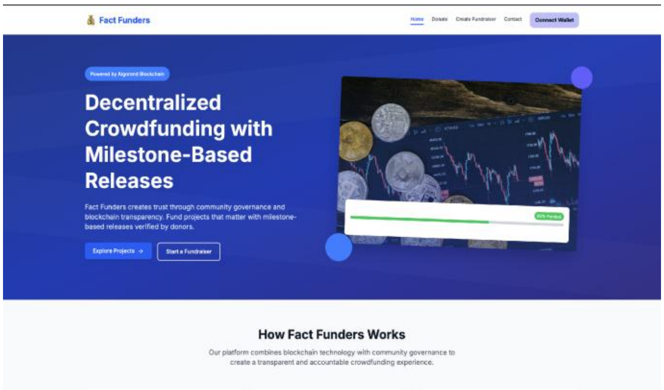

Fig -2: Landing Page of the Fact Funders Platform

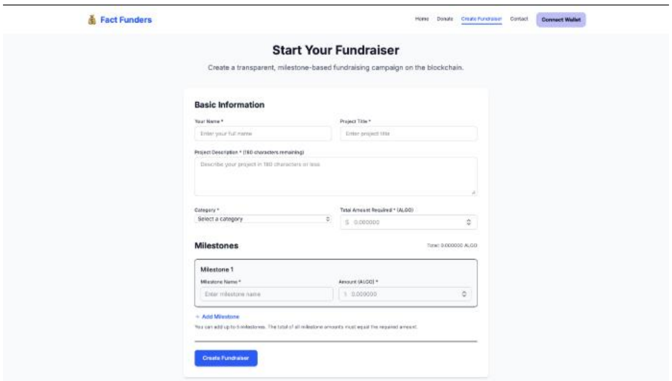

Fig -3: Fundraiser Creation Interface with Milestone Configuration

Table -1: Average Transaction Costs on Algorand TestNet

Function	Avg. Cost (Algos)	Avg. Cost (USD, est.)
create_proposal	0.001	< 0.01
donate_proposal	0.001	< 0.01
submit_proof	0.001	< 0.01
vote_milestone	0.001	< 0.01
claim_milestone	0.001	< 0.01
refund_if_inactive	0.001	< 0.01

5.1 Transaction Costs

Transaction fees are critical for determining the feasibility of blockchain-based crowdfunding. Table -1 summarizes the costs observed during experiments.

The results confirm that Fact Funders is viable for micro-donation scenarios. Algorand allows donors to contribute as little as 1 Algo without fees undermining their value.

5.2 Latency and User Experience

Transaction latency, measured as the time between submission and confirmation, averaged between 4–6 seconds. This is consistent with Algorand TestNet block times and provides a near-real-time experience for users. For crowdfunding contexts, such delays are acceptable, as campaign events (donations, votes, disbursements) do not require millisecond-level responsiveness.

During peak TestNet congestion, delays extended to 10–12 seconds in rare cases. While not disruptive, this highlights the importance of Algorand's high-throughput design for scaling to larger ecosystems.

5.3 Governance Fairness Analysis

A central innovation of Fact Funders is the integration of square-root weighted voting. To evaluate fairness, we simulated various donor distributions and analyzed outcomes.

1) Scenario 1: Equal Donors-3 donors, each contributing 3 Algos. Weights: $\sqrt{3} \approx 1.73$ each. Outcome: equal influence, aligning with fairness expectations.
2) Scenario 2: Unequal Donors-1 Algo, 4 Algos, 9 Algos. Weights: $\sqrt{1} = 1$, $\sqrt{4} = 2$, $\sqrt{9} = 3$. Outcome: larger donors held more influence but not linearly proportional. The 9-Algo donor had 3x the influence of the 1-Algo donor, not 9x, balancing proportionality with fairness.
3) Scenario 3: Whale Donor vs. Many Small Donors-one donor with 25 Algos, ten donors with 1 Algo each. Weights: whale = $\sqrt{25} = 5$; each small donor = $\sqrt{1} = 1$. Outcome: small donors collectively outweighed the whale (10 vs. 5). This demonstrates that coordinated smaller contributors can still control governance outcomes.

Square-root weighting mitigates plutocracy risks inherent in purely token-proportional systems while preserving proportional influence, fulfilling governance objectives.

5.4 Summary of Findings

The results of experimental evaluation confirm that Fact Funders achieves its design objectives:

- functional correctness across all contract operations;
- extremely low transaction costs suitable for micro-donations;
- near real-time transaction confirmation with 4–6 second latency;
- governance fairness through square-root weighted voting;
- strong donor protection via proportional refunds;
- scalability for multiple concurrent campaigns.

Ultimately, Fact Funders demonstrates that blockchain-enabled governance can provide a more accountable, transparent, and donor-centric model of crowdfunding, addressing key shortcomings of both traditional platforms and earlier decentralized models.

6. CONCLUSION AND FUTURE SCOPE

This paper introduced Fact Funders, a decentralized crowdfunding platform built on the Algorand blockchain to address long-standing issues in crowdfunding such as lack of accountability, risk of project abandonment, and inequitable governance. By leveraging Algorand's efficient consensus protocol and ARC4 smart contracts, the system integrates three key mechanisms: milestone-based fund disbursement, square-root weighted donor governance, and inactivity-triggered refunds. Together, these features ensure that funds are distributed only when verified progress is achieved, donors maintain a meaningful role in governance, and unspent contributions are protected. Experimental validation confirmed that Fact Funders delivers cost efficiency, scalability, and transparency, positioning it as a viable alternative to both centralized platforms and earlier blockchain-based crowdfunding models.

Looking forward, Fact Funders opens promising avenues for further research and refinement. Integration with Decentralized Identity (DID) could improve accountability by linking creators to verifiable credentials, while reputation systems could reward reliable actors. Additionally, donor participation incentives such as tokenized rewards or reputation points could strengthen voter engagement and governance robustness. Finally, exploring policy and regulatory compliance, including KYC and AML frameworks, will be crucial for mainstream adoption. By addressing these future directions, Fact Funders can evolve into a more comprehensive and widely trusted decentralized funding ecosystem.

REFERENCES

[1] T. Aste, P. Tasca, and T. D. Matteo, "Blockchain technologies: The foreseeable impact on society and industry," Computer, vol. 50, no. 9, pp. 18–28, 2017.

[2] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," in Proc. IEEE 18th Int. Conf. e-Health Networking, Applications and Services (Healthcom), Munich, 2016, pp. 1–3.

[3] S. B. Baker, W. Xiang, and I. Atkinson, "Internet of things for smart healthcare: Technologies, challenges, and opportunities," IEEE Access, vol. 5, pp. 26521–26544, 2017.

[4] T. Ahmad, M. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "Overview of 5G security challenges and solutions," IEEE Communications Standards Magazine, vol. 2, no. 1, pp. 36–43, Mar. 2018.

[5] T. Kumar, M. Liyanage, I. Ahmad, et al., User Privacy, Identity and Trust in 5G. Hoboken, NJ, USA: Wiley, 2018.

[6] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," in Proc. Int. Conf. Open and Big Data (OBD), Vienna, Austria, 2016, pp. 25–30.

[7] T. Kumar, A. Braeken, M. Liyanage, and M. Ylianttila, "Identity privacy preserving biometric based authentication scheme for naked healthcare environment," in Proc. IEEE Int. Conf. Communications (ICC), Paris, 2017, pp. 1–7.

[8] T. Kumar, M. Liyanage, A. Braeken, I. Ahmad, and M. Ylianttila, "From gadget to gadget-free hyperconnected world: Conceptual analysis of user privacy challenges," in Proc. European Conf. Networks and Communications (EuCNC), Oulu, 2017, pp. 1–6.

[9] P. Zhang, M. A. Walker, J. White, and D. C. Schmidt, "Metrics for assessing blockchain-based healthcare decentralized apps," in Proc. IEEE 19th Int. Conf. e-Health Networking, Applications and Services (Healthcom), 2017.

[10] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control," Journal of Medical Systems, vol. 40, p. 218, 2016.

[11] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where is current research on blockchain technology? A systematic review," PLOS ONE, vol. 11, no. 10, 2016.

[12] M. Bartoletti and L. Pompianu, "An empirical analysis of smart contracts: Platforms, applications, and design patterns," Univ. degli studi di Cagliari, 2017.

[13] C. Wright and A. Serguieva, "Sustainable blockchain-enabled services: Smart contracts," in Proc. IEEE Int. Conf. Big Data, Boston, MA, 2017, pp. 4255–4264.

[14] T. Nugent, D. Upton, and M. Cimpoesu, "Improving data transparency in clinical trials using blockchain smart contracts," F1000Research, vol. 5, 2016.

[15] M. Benchoufi, R. Porcher, and P. Ravaud, "Blockchain protocols in clinical trials: Transparency and traceability of consent," F1000Research, vol. 6, p. 66, 2017.

[16] M. Benchoufi and P. Ravaud, "Blockchain technology for improving clinical research quality," Trials, vol. 18, p. 335, 2017.

[17] K. A. Clauson, et al., "Leveraging blockchain technology to enhance supply chain management in healthcare," Blockchain in Healthcare Today, 2018.

[18] M. A. Engelhardt, "Hitching healthcare to the chain: An introduction to blockchain technology in the healthcare sector," Technology Innovation Management Review, vol. 7, no. 10, 2017.

[19] M. N. K. Boulos, J. T. Wilson, and K. A. Clauson, "Geospatial blockchain: Promises, challenges, and scenarios in health and healthcare," Int. J. Health Geographics, vol. 17, p. 25, 2018.

[20] M. Puppala, T. He, X. Yu, S. Chen, R. Ogunti, and S. T. C. Wong, "Data security and privacy management in healthcare applications and clinical data warehouse environment," in Proc. IEEE-EMBS Int. Conf. Biomedical and Health Informatics (BHI), Feb. 2016, pp. 5–8.

[21] A. Al Omar, M. S. Rahman, A. Basu, and S. Kiyomoto, "Medibchain: A blockchain-based privacy preserving platform for healthcare data," in Int. Conf. Security, Privacy and Anonymity in Computation, Communication and Storage, 2017, pp. 534–543.

[22] G. Zyskind, O. Nathan, and A. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in Proc. IEEE Security and Privacy Workshops, San Jose, CA, 2015, pp. 180–184.

[23] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "MeDShare: Trust-less medical data sharing among cloud service providers via blockchain," IEEE Access, vol. 5, pp. 14757–14767, 2017.