# Review of: "A Proposed Secure Wearable Device Payment System Based on Blockchain Technology"

Ahmed Gad[1]

1 Faculty of Computers and Information, Kafr El-Sheikh University, Egypt

Potential competing interests: No potential competing interests to declare.

The manuscript explores the integration of blockchain technology with IoT-based wearable devices for secure financial transactions. It identifies security vulnerabilities in current wearable payment systems and proposes a blockchain-based framework to address issues such as data integrity, user anonymity, and protection against attacks. The paper includes a comprehensive literature review covering blockchain, IoT, and wearable devices, and presents a conceptual framework for the proposed system. However, the research remains largely theoretical, lacking empirical validation or practical implementation, and raises concerns about scalability, technical depth, and real-world applicability.

## Strengths:

**Relevance and Timeliness**: The paper addresses a highly relevant topic—the integration of blockchain technology with wearable devices for financial transactions. This is particularly timely given the increasing reliance on decentralized systems in the fintech sector, where security and transparency are paramount. The topic holds substantial potential to impact both IoT-based payment systems and blockchain applications in real-world use cases.

**Clear Problem Identification**: The paper identifies security vulnerabilities in IoT-based wearable payment systems and presents blockchain as a viable solution to address these concerns. This makes the research problem clear and aligns with the current needs of the fintech and IoT sectors.

**Well-Organized Structure**: The paper's structure, including sections dedicated to the literature review, system architecture, and proposed solutions, is clear and methodical. This allows the reader to follow the logical progression of the argument easily.

**Broad and Comprehensive Literature Review**: The literature review is thorough, offering extensive coverage of relevant work on blockchain, IoT, and wearable devices. It effectively establishes the groundwork for the research and contextualizes the proposed solution within the existing body of knowledge.

**Innovative Conceptual Framework**: The integration of blockchain into wearable payment systems represents a novel approach that could enhance security, making the conceptual framework one of the paper's key contributions. The focus on IoT-related challenges further emphasizes the innovation in applying blockchain technology in this niche.

## Weaknesses:

**Theoretical Nature of the Proposed System**: One of the primary limitations is the lack of empirical validation for the proposed system. While the framework is conceptually sound, its efficacy remains theoretical without a prototype or experimental data. Providing real-world testing or simulation results could significantly strengthen the impact of the research.

**Insufficient Practical Detail on Blockchain Implementation**: The technical explanation of blockchain in the paper is somewhat generalized. A more detailed discussion on how blockchain will address specific security vulnerabilities in IoT, such as denial-of-service attacks, data breaches, or key management, would enhance the technical depth. Furthermore, details on how blockchain improves efficiency or usability in wearable payment systems are minimal.

**Scalability Challenges**: While the paper acknowledges scalability as a challenge in IoT systems, there is insufficient discussion on how the proposed blockchain solution will handle large-scale deployment. Providing a more detailed analysis of blockchain's potential limitations—such as processing overhead, transaction speed, and energy consumption on wearable devices—would enhance the paper's comprehensiveness.

**Unclear Contribution of the Work**: The unique contribution of the research, beyond a detailed literature review and conceptual framework, is not sufficiently highlighted. The paper could do more to clarify how its proposed solution advances the current state of research, particularly in terms of improving security, usability, or efficiency in real-world applications.

**Methodological Weakness**: The paper lacks a detailed research methodology, which weakens its overall structure. There is no clear explanation of how the proposed solution was developed or validated. Including a clear methodology—whether experimental, simulation-based, or comparative—would enhance the rigor of the study.

**Limited Results and Analysis**: The absence of practical results or detailed performance analysis reduces the paper's effectiveness. A comparison between the proposed system's performance (in terms of security, transaction speed, or scalability) and existing solutions would add significant value.

## Recommendations for Improvement:

**Empirical Validation or Simulation**: To make the proposed solution more convincing, the paper should include empirical testing, a working prototype, or at least a simulation of the blockchain-based wearable payment system. Performance metrics such as latency, throughput, energy consumption, and security handling in real-world scenarios would substantiate the theoretical claims made.

**Clarify Contributions**: The paper's contributions need to be explicitly stated, distinguishing the proposed solution from existing literature. Focus on what sets this work apart, such as specific enhancements in security or efficiency, or how the proposed system addresses gaps not covered by previous research.

**Strengthen the Conceptual Framework**: The conceptual framework should be expanded with more detailed descriptions of each layer, along with their respective roles in the system. Comparing this framework with similar ones from the literature could offer insights into its advantages and limitations, adding to the clarity and thoroughness of the work.

**Scalability and Efficiency Considerations**: Future versions should address how the proposed system can scale while maintaining efficiency. Discussing potential optimizations or solutions for the energy consumption of wearable devices running blockchain algorithms would be useful. The paper could also explore alternative solutions, such as hybrid systems, to complement blockchain.

**Refine Technical Explanations**: A more technically in-depth explanation of how blockchain will mitigate specific IoT vulnerabilities—such as encryption, key management, and network attacks—would strengthen the paper. Providing case-specific security mechanisms, rather than general benefits of blockchain, would add robustness to the argument.

**Methodology Section**: Introducing a well-defined methodology that outlines the steps for designing, implementing, and testing the proposed system is crucial. If an implementation is not feasible at this stage, a detailed simulation approach or algorithm description could be included instead.

**Language and Presentation**: Minor issues with language and terminology can be improved, particularly in the abstract and introduction sections. Correcting phrases such as “security dangers” to “security threats” and ensuring consistent use of formal research language would enhance readability.

By incorporating these changes, the paper will be more complete and impactful, offering a stronger contribution to the fields of IoT, wearable devices, and blockchain technology in financial transactions.