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

Anas Abou El Kalam[1]

1 Cadi Ayyad University, Marrakesh, Morocco

Potential competing interests: No potential competing interests to declare.

After thoroughly reviewing your manuscript, I find your work on a proposed secure wearable device payment system based on blockchain technology relevant and timely, especially given the increasing adoption of wearable technologies in financial services. However, while your conceptual framework offers valuable insights, the paper must significantly improve clarity, depth, and practical application.

Firstly, although you propose a blockchain-based architecture, the technical details of the system could be more developed. The architecture is presented at a high level without sufficient elaboration on how blockchain will be specifically integrated into the wearable payment system. Key aspects such as encryption protocols, transaction validation, and management should be addressed more deeply. Due to their limited computational resources, wearable devices may face significant challenges in implementing blockchain-based protocols, and your paper would benefit from a more detailed explanation of how these challenges will be managed. A notable gap is the lack of clear explanations regarding the choice of blockchain (e.g., public vs private consensus mechanisms) and how these will affect transaction throughput, latency, and device resource consumption. While the paper presents the idea of blockchain as a solution, more technical rigor is needed to demonstrate its feasibility in this context.

Additionally, while you highlight scalability as a key issue in IoT networks, the paper needs to address how your proposed system will overcome the inherent scalability challenges of blockchain technology itself. As is well-known, blockchain needs faster transaction processing speeds and incurs higher costs as the network grows, particularly in its public form. There needs to be a discussion of potential solutions to this problem, such as Layer 2 solutions or sidechains, which could improve scalability while maintaining security. This omission raises concerns about the practical viability of your system, especially when considering real-time financial transactions, which demand low-latency processing.

Moreover, the security mechanisms in your paper could be expanded significantly. While the paper briefly mentions elliptic curve cryptography (ECC) and blockchain's inherent cryptographic features, there needs to be more detail on how these technologies will be implemented within the wearable ecosystem. You mention using blockchain to secure financial transactions. Still, there needs to be more elaboration on how specific security threats, such as man-in-the-middle (MitM) attacks, replay attacks, or device tampering, will be mitigated. Discussing attack vectors could be enhanced by considering wearable devices' limited capabilities and how blockchain, particularly transaction validation and consensus mechanisms, will address these concerns without overloading the device.

Another area that needs attention is the need for real-world validation. The paper proposes a system, but a prototype, simulation, or real-world case study needs to be used to demonstrate the feasibility and performance of the system. Including such an evaluation would significantly strengthen the contribution of your paper, offering concrete evidence of the system's practicality. It is also important to note that without any performance benchmarks or a simulation environment, assessing how well your proposed system will function in terms of transaction speed, scalability, and security is difficult.

Additionally, the writing style and presentation of the paper would benefit from more careful editing. Numerous grammatical errors and unclear sentences detract from the paper's readability. For example, the section "Conclusion and Suggestion for Future Studies" could be rephrased for better clarity and flow. A thorough proofreading would help improve the overall readability and professionalism of the manuscript.

In conclusion, while your paper addresses a pertinent issue and proposes an interesting solution, it needs more technical detail, security analysis, and real-world validation to support its claims. I would recommend a substantial manuscript revision that includes a more detailed technical breakdown of the system architecture, specific methods to address security and scalability concerns, and, ideally, a prototype or simulation to demonstrate the system's feasibility in practice.