v1: 1 October 2024

Research Article

A Proposed Secure Wearable Device Payment System Based on Blockchain Technology

Preprinted: 18 September 2024
Peer-approved: 1 October 2024

Qeios, Vol. 6 (2024)
ISSN: 2632-3834

Maimunatu Ya'u Ibrahim [1], Kabiru Ibrahim Musa[1], Aminu Ahmad[1], Yakubu Yarima[1]

1. Faculty of Management Sciences, Department of Management and Information Technology, Abubakar Tafawa Balewa University, Nigeria

Given that they are employed in several services, wearable technology is growing in popularity. The wristwatch gathers several types of personal information. Consumers may find gadgets convenient, but there are also security dangers that alert users to the possibility of cybersecurity breaches, device intrusions, and vulnerability exploitation. Hacking may make the collected data visible since devices are vulnerable to assault. Issues with these devices include security flaws, Bluetooth troubles, and the absence of authentication and location tracking. The Internet of Things (IoT) includes wearable gadgets as cogs in the wheel that might have an effect on the banking and financial industries. Therefore, since blockchain technology has gained a lot of attention recently and is now one of the most popular ways to securely transfer data through decentralised peer-to-peer systems, it is imperative to employ its security capabilities on the existing IoT-based wearable payment system. A secure, decentralised transaction execution process is made possible by blockchain, an unchangeable ledger. It has a great reputation and more customers thanks to its complex yet safe technique. Based on blockchain technology, this research suggested a secure wearable device payment system.

Correspondence: papers@team.qeios.com — Qeios will forward to the authors

Introduction

Industry 4.0 is a revolutionary concept that improves business intelligence, efficiency, and communications by fusing smart technologies, big data analytics, blockchain, artificial intelligence, and the IoT. Almost all company procedures can be modified using the IoT, and it may also provide new business opportunities. Thanks to Industry 4.0 technology, businesses now have new opportunities to collect, analyse, and apply data to boost their production and efficiency. Modern technology helps businesses by saving money, time, and reducing defective products. Both industrial processes and service sectors like banking and accounting have benefited from the widespread deployment of Industry 4.0 technology to boost productivity and efficiency[1].

More research has been done on the use of IoT-based technologies in innumerable industries. IoT technology's influence on service-oriented business

doi.org/10.32388/K2VI7Z.2

models is, however, the subject of few researches. The banking industry and the financial technology (FinTech) industry have not been exempted from the valuable applications that the IoT has brought to a range of businesses[2]. The IoT is a constantly and increasingly prevalent technology that has developed with global computing in today's technological era. Instances of IoT uses that have improved people's lives include smart homes, smart cities, and smart transportation[3]. However, it's been discovered that security is a major issue that has prevented IoT from being widely used. The banking industry and the FinTech industry have seen several significant changes that have advanced their procedures during the past several decades. Currently, banks around the world have efficiently used smart technologies such as artificial intelligence, IoT, and information and communication technology as strategic devices to enhance speed, effectiveness, competitive advantages, and reduce costs[4].

One new idea that incorporates wearable technology is the IoT, as we all know, is all about connecting objects to improve lives, boost productivity, and save expenses. Payment systems are fundamentally based on wearable technology. It is essential to Nigeria's banking and FinTech sectors. The significance and enormous influence that wearable technology has had over the last five years in illustrating the exponential growth in wearable payment transactions are being acknowledged by more and more studies. As a result, banks and FinTech are providing their clients with an increasing array of features and practical services, such as stock purchases, payments, and notifications. These banking and financial applications make advantage of wearable sensor devices, such as smart watches, smart jewellery, smart glasses, smart uniforms, etc[5].

The security of the IoT payment device itself, data leakage, and privacy due to IoT devices' inherent poor resilience to data leakage, and distributed denial of service (DDoS) attacks are some of the significant security risks that need to be addressed. Denial of service (DoS) attacks, malware, and jammer assaults are just a few of the cybersecurity issues that IoT users must deal with[6]. One well-known type of attack against IoT devices is DDoS assaults; since sensors and radio frequency identifiers (RFIDs) are the primary data collection devices, jamming, killing instructions, and de-synchronizing attacks are essential to DDoS attacks[7].

The adoption of decentralised systems has made creative methods for decentralisation, security, immutability, audibility, and transparency possible. The provenance notion is satisfied by decentralised data storage as it preserves historical records and inhibits record modification. Decentralised methods are therefore more suitable for wearable banking payment systems. Customers in several domains have been drawn to blockchain technology and have been compelled to abandon the centralised cloud strategy in favour of a blockchain-based one[8]. As a result, blockchain technology solves the scalability issues and intermediate weaknesses in micropayment channels, making it safe and unchangeable. Therefore, in order to perform safe IoT digital banking payments, these linked IoT devices and payment systems must comply with it[9]. PWC estimates that by 2030, blockchain technology may boost global economic growth by up to $1.76 trillion[10].

This study seeks to propose a secured wearable device payment system using blockchain technology. Global payments have been greatly impacted by wearable payments. The FinTech and banking businesses receive a variety of benefits from wearable technology. The gadgets depend on many wireless message protocols that support many different communication ranges[11]. Through the establishment of secure SSL/TLS connectivity, additional wearable devices and wearable sensors will convey critical data to phone user apps[12]. Banking and financial transactions require SSL/TLS communication, made possible by collective authentication and later generations of session keys[13]. However, application developers face a difficult problem when working with SSL/TLS. Wearable communication opens the door to various well-known attacks, including man-in-the-middle (MitM), replay, mobile or handheld terminal theft, device tampering, eavesdropping, etc.

Therefore, by recording in what way devices interact, blockchain can help solve most security holes and traceability issues in financial transactions. What are they, and how do they interact with other IoT devices in this state? For enhanced data security, a blockchain is hack-resistant and has minimal risk of compromise[14].

Statement of the Problem

IoT devices are a popular target for attackers because they usually have security weaknesses. As a result, financial institutions are in disarray due to several attacks[3]. Cybercriminals may utilize unsecure IoT devices as a convenient target by launching cyberattacks using the devices′ lax security[3]. Scalability is another issue with current IoT networks. As the number of devices connected via the IoT network increases, the bottleneck will be caused by the existing centralized processes used to attest, authorize, and connect the various nodes in the network. Therefore, it is imperative to tackle the safety and scalability challenges in monetary dealings, given that IoT devices are expected to become an important part of daily routine in the coming years[15].

An ″elliptic curve integrated encryption system (ECIES)″ is used by Bojjagani, et al.[16] as a security mechanism to encode and decode the shared communications amongst several individuals in their payment model architecture for wearable devices. Elliptic curve cryptographic systems are public-key techniques that enable key exchange, encryption, and digital signatures. The user password is encrypted using a ″public key″ as the foundation of the security system. However, regardless of the numerous benefits of elliptic curve cryptography, there is one big drawback: difficulty in sending the keys needed to encrypt and decrypt data. These keys are easily intercepted by malicious third parties when transmitted over an unsecured connection. The security of any data encrypted with a public key is compromised if an unauthorized person gains access to that key. Thus, the security and scalability challenges of IoT can be helped by blockchain technology[15].

In light of the above, blockchain′s distinct benefits and capabilities make it a game-changer for information. The asymmetric cryptographic method used in the blockchain-based payment system will be beneficial in helping to overcome the authentication challenge. Two cryptographic keys, the public key and the private key, will be stored on each node. Everyone who wants to convey encoded documents with the possessor of the private key can get the public key. The key objective of this paper is to propose a secure wearable device payment system using blockchain technology. To achieve this, the subsequent definite aims are proposed: To propose a design, development, and implementation of a blockchain-based wearable device payment system.

Literature Review

The term IoT was originally used in 1999 by the Radio Frequency Identification (RFID) Association, led by member Kevin Ashton, to describe a future in which everything will have digital individuality and be able to be managed and arranged by computers, even inanimate objects. The concept has proven successful in the near term because of the increasing prevalence of mobile devices and the growing popularity of computing, data analytics, and communication[17]. A network of connected computers, digital gadgets, and sensors that can share data without interacting with other devices is known as an IoT system[18]. Data processing, user interfaces, communication, and sensors/devices make up its four main parts. IoT systems in real life connect to the cloud and utilise data analysis to make decisions. Some examples of these decisions include notifying users or automatically adjusting sensors or equipment[19]. Connecting online social networks and autonomous resource distribution, as well as enabling intelligent objects to communicate and make decisions on their own without human intervention, are the two main goals of the IoT, a revolutionary paradigm that links online social networks with the physical and social environment[20].

The IoT is one of the key technologies underlying Industry 4.0 and the fourth industrial revolution[21]. IoT systems and devices have the potential to detect, collect, and store enormous amounts of data for subsequent analysis by other connected devices. Generally speaking, data processing occurs on cloud-based centralised servers Chen et al.,[22] that are powered by the newest, most dependable methods to ensure peak performance, including edge computing, mobile cloud computing[23], and energy harvesting[24]. The results may then be used at other decision-making levels and facilitate real-time communication with other sectors and supply chain partners[25].

The IoT may be advantageous for supply chains, manufacturing, healthcare, transportation, energy, and other industries[26][27]. IoT offers a lot of potential benefits, but there are also many problems and limitations that need to be worked out. Among these challenges and limitations are security and privacy[28], communication, hardware and software, IoT-related skill sets, legislation, law, and culture[29]. As the name suggests, Bluetooth, Near-Field Communication (NFC), Long Term Evolution (LTE), Wireless Sensor Networks (WSN), Radio-frequency identification (RFID), and other smart communication technologies are used to link objects to the Internet. Consequently, IoT may be defined as "things that are associated over the Internet". Information delivered from various devices via the Internet to its intended destinations is made easier by this link[30]. The standard of living in our society has radically altered as a result of modern technologies. This is often because of developments in communication and semiconductor technologies, which allow for device networking and alter the nature of human-machine connectivity. IoT is the term commonly used to describe this evolution[31].

The fast growth of smart devices and high-speed networks has led to the widespread recognition and popularity of IoT, since it makes use of the low-power lossy networks (LLNs) standard. These LLNs may utilise the limited resources by utilising comparatively little electricity. IoT devices may be remotely configured to perform a certain function. Data exchange between devices is facilitated by the network through the use of standard communication protocols. According to Sultan et al.[32], the networked "things" come in a variety of sizes, from tiny wearables to large machines equipped with detector (Sensor) chips. Data from IoT devices are processed by a gateway before being sent over the internet to remote servers, clouds, or data centres for software applications. A variety of sensing device nodes are combined in an IoT system to collect data from clients and the actual world[33]. These software applications, which are developed in response to customer demands for services ranging from retail to corporate, are kept in data centres. The IoT consists of three tiers. The network transmission layer appears first, followed by the perception layer and the application layer. The collected data and associated information may be thoroughly examined and used in light of the first two levels[34].

Smart grids, smart houses, smart monitoring, environmental monitoring, and other domains are among the common IoT applications. IoT is showing promise in certain sectors of the economy, but many bankers are still figuring out how this technology might help the sector, which depends mostly on intangible assets, like banking. The two primary IoT prospects for banks are to: (1) directly utilise sensor data to evaluate dependability; and (2) collaborate with manufacturers of goods that use sensors to offer payment services for transactions conducted with devices[35]. The following is a list of typical IoT designs[36]. The expansion of remote banking services through different communication channels in the banking and financial services sector has helped to provide customers with a new type of added value. With the broad use of smartphones, especially for additional wireless devices such as wearables and sensors, IoT has become a logical breakthrough in e-banking. Prospective IoT applications in these industries comprise worker's compensation, lifetime and health indemnity, investment management, and telematics insurance. Undoubtedly, IoT will improve the customer experience and the overall network infrastructure of banks. While online and mobile banking systems currently provide customers with generally good services, the implementation of IoT technology can improve service quality[37]. Wearable technology has become an indispensable component of payment systems and plays a crucial role in the banking and FinTech sectors in Nigeria. Over the last five years, wearable technology has demonstrated exponential growth in wearable payment transactions, and this has led banks and FinTech to provide their customers with an increasing array of convenient services and features, such as stock purchases, notifications, and payments[38].

Top innovations in the banking sector include, but are not limited to:

- **Banking on wearables:** Wearable technology has, up till now, been the most important bank technology because of a developing biological system of devices and a usually simple start. Credit cards may now be used with Fit Pay and Apple Watch applications, according to several banks. Many banks use their own wristbands to offer certain contact-free instalments[39].
- **Proactive service:** The ability of financial and monetary administrations to promptly change financial product or administration choices will be greatly improved by IoT. Let's say anything is the subject of any doubt or concern. In this case, the issues are easy to spot and may be resolved as soon as practical. Advisors are also willing to share examples from the past with clients and manage them correctly. Modern accounting technology advancements can improve firm operations[40].

- **Banking at home:** Although Capital One is now the only retail managing account association in the United States to provide this service, it won't be the last. Customers may use Amazon's Alexa to pay their bills through Capital One. Consider the Google Home project by UK challenger bank Starling, which combines a smart speaker with their API to let consumers voice-directly bring up balance issues and instalments[41].

Studies on wearable devices payment system

Ramos de Luna et al.[42] looked at whether or not NFC technology was used for mobile payments. The findings demonstrate that mindset, individual IT innovation, and perceived utility are factors that influence future intentions to employ NFC technology for payments in Brazil. Liébana-Cabanillas et al.[43] to examine customers' inclination to utilize SMS and NFC mobile payment systems, researchers combined subjective standards and perceived security with TAM characteristics (such as perceived utility, perceived simplicity of use, and attitude). The results demonstrated that perceived utility, perceived usability, perceived ease of use, subjective norms, and perceived security are major determinants of behavioural intention; nevertheless, attitude was the most significant determinant of users' intention to use various payment methods. In order to explore the factors that influence the acceptability of NFC-based mobile payments in the restaurant business, Khalilzadeh et al.[44] integrated TAM and UTAUT. The study's findings provided compelling evidence of how risk, security, and trust affect consumers' willingness to utilize NFC-enabled mobile payments. Additionally, while taking into account the overall impact, attitude, security, and risk have the greatest impact on customers' behavioural intentions. The study's findings also showed that effort expectation, hedonic and utilitarian performance expectancy, attitude, and intention are additional crucial factors having direct and indirect effects on risk, security, and trust.

The adoption of NFC m-payments in public transportation, as well as the variables influencing consumers' intentions to keep using this technology, were examined by Liébana-Cabanillas et al.[45]. The findings demonstrated that factors affecting the continuous desire to use this payment method include satisfaction, service quality, effort expectations, and perceived risk. However, consumers' happiness was unaffected by perceived trust, social value, and ease.

In order to better understand the elements that influence customers' decisions to embrace NFC m-payments, Zhao et al.[46] expanded TAM with financial incentives and perceived risk. According to their research, customers' intentions to use NFC m-payment were indirectly impacted by perceived risk rather than directly by the presence of financial incentives.

Customers' individual characteristics and their intentions to adopt NFC-based mobile payments in restaurants were examined by Esfahani and Ozturk in 2019[47]. The results showed that customers' intentions to utilize NFC mobile payments at restaurants varied significantly depending on their prior experiences, age, and gender.

Zhang et al.[48] also looked into how consumer characteristics affected consumers' inclinations to use NFC mobile payments. The findings demonstrated that individual behavioural intentions were highly influenced by relative advantage, attitude, and subjective norms. In order to examine the effects of perceived aesthetics, technology readiness, mobile usefulness, and mobile ease of use on behavioural intention to adopt wearable payments, Lee et al.[49] integrated the Mobile Technology Acceptance Model (MTAM)[50] with Fashion Theory (i.e., perceived aesthetics) and Technology Readiness Theory. The study's findings showed that every factor was relevant in predicting consumers' inclination to utilize this payment option.

Studies on IoT

Kumar et al.[51] developed an authentication technique for wearable devices using elliptic curve cryptography (ECC). This technique provides a formal verification, even when real-time implementation scenarios are not verified. Moreover, it cannot establish secure connections between servers and IoT devices, or between various organisations and application providers. Magdum et al.[52] introduced a unique contactless transaction system for wearable devices with a biometric fingerprint feature; the authors did not give any proof of wearable payment implementation in real time, but they did describe phases for the protocol's execution flow.

An innovative IoT-based micropayments mechanism was presented by Bojjagani et al.[16] The device informs the smartphone, which then gets word to the banks about the payment request. The method, however, is only applicable to small transactions; it might not function if the user mixes wearable technology with online banking or a credit card. A number of the findings in related schemes, such as the fact that most techniques pair devices over Bluetooth—which is currently unsafe for payments—are made. The associated efforts do not succeed in creating apps for real-time implementation. Most of the programs don't deal with payments made using wearables. While some payment methods are supported, only particular payment types can use them.

Furstenau et al.[53] looked at the main problems with IoT from a network standpoint. The following concerns are raised: internet, sensor networks, network imbalance, mobile assistance, and security. Alotaibi[54] spoke about how, as IoT technologies evolve, every gadget we use on a regular basis is becoming increasingly connected. These systems have the ability to link and communicate with both their surroundings and one another in order to carry out their duties. For the sake of security, dependability, suitable authentication, and, ultimately, basic maintenance services, these systems must be connected. To provide all of these functions, blockchain will be required. Our current IoT-based payment systems have several security, authentication, and maintenance issues; yet, their decentralised design may be the solution.

Hang and Kim[55] talk about how the IoT is becoming used in the financial sector and how its popularity is growing. Unfortunately, the processing power, storage capacity, and network bandwidth of these IoT network devices are limited. For this reason, they are more vulnerable than other endpoints, such as a smartphone. Additionally, as these devices become more widespread, the computer architecture of these devices becomes more intricate. This might result in cyberattacks. Due to its many capabilities that may be applied to solve a range of issues that IoT network devices face, blockchain has lately gained prominence. Blockchain uses a distributed database to track records. It contains proof of each task that network nodes have finished.

The challenges and current solutions in IoT security research have been presented by Dai et al[56]. They have also highlighted issues that still need to be addressed and provided some suggestions for next advancements. In order to address privacy and trust issues, access control and confidentiality in IoT applications, and policy enforcement in IoT applications, the research looks at and summarises existing approaches. Given the plethora of unanswered questions our study raises, additional IoT security research is needed. According to the research and survey the authors conducted for this work, appropriate solutions must be developed and prepared in order to provide confidentiality, dependability, and access control.

The functioning of blockchain technology and smart contracts in the IoT has been studied by Sultan et al.[32] They have given a comprehensive explanation of the operation of a blockchain network, including the interactions between transacting parties. Furthermore, the writers have demonstrated how the blockchain with IoT might facilitate service sharing among users, perhaps leading to the creation of a device-to-device marketplace.

Hassan et al.[57] set out to present a detailed examination of the features and security issues of the IoT in this article in order to understand the dispersed approach of the IoT and its role in the future of the internet. Among other challenges, creating a business model, managing entity authorisation and authentication, and ensuring interoperability are all necessary. But there are also a number of benefits. Since intelligence is not limited to a few centralised application platforms—even if these platforms could still exist to offer further support—scalability is increased.

Studies on Blockchain Technology

According to Deepak et al.[58], a blockchain may be employed in several study domains to thwart attacks on centralised organisations such as cloud, IoT, and big data. Stefan[59] argues that while experts anticipate blockchains to be used in banking, there aren't nearly enough real-world uses for them in contemporary culture. Tejal and Shalilak[60] assert that the blockchain has the power to lower costs, eliminate the need for middlemen, and increase banking industry profitability. A private blockchain enables transactions to happen faster and with more security. This new technology will save costs and streamline banking procedures.

Tejal and Shalilak[60] suggest that blockchain technology might assist the banking industry in eliminating intermediaries, reducing costs, and increasing revenues. Transactions on a private blockchain are faster and more secure. This invention will save costs and streamline banking operations. Lawrence[61] outlines a few of the problems that are driving the rapid progress of technology in the financial services industry. According to Tejal and Shalilak[60], the blockchain has become the most important tool in the fight for financial inclusion. Ittay[62]'s author investigates how and why blockchain has developed into the financial technology sector's puppet.

Fakhri and Mutijarsa[63] address blockchain technology-based secure IoT connectivity in their study. IoT growth is also contributing to a rise in security difficulties because of several security policy violations. Blockchain can address any issue related to IoT security. One way is to establish secure communication between all the devices. In order to illustrate the importance of blockchain, they created two IoT systems, one with and one without blockchain. Two protocols are used for communication: MQTT and Ethereum. They have evaluated both systems by tracking the outcomes and emulating attacks. They proved through several trials that the blockchain-powered IoT system was better and could address security concerns.

In this paper, Alotaibi[54] has emphasised recent advancements in security to solve IoT limits through the use of blockchain. The author has demonstrated how the blockchain seeks to overcome the cybersecurity limitations of IoT. As a result, they may be divided into four groups: confidentiality, data integrity, and availability (CIA); identity verification and authentication; data privacy and anonymity; and end-to-end traceability. This essay also looks at systematic techniques that can be useful. Effective IoT applications and approaches (those related to cybersecurity) are examined in order to show how cutting-edge technologies like blockchain and IoT could, in fact, be highly beneficial. Lastly, a synopsis of the likely roadblocks to blockchain and IoT integration is given.

All of the data that this telemetry system gathers is transferred remotely to the decentralised crypto-hash database, where it is updated dynamically based on acceptance from around 75% of the members of the chain agreement. A decentralised, service-oriented universal computing paradigm was developed by White et al.[64] with the aim of monitoring public road travel. With the purpose of improving traffic safety, managing transportation networks, providing passengers with real-time information, and managing data on public transportation networks, this system is an intelligence-based, service-oriented utility.

Jeong and Ahn[65] produced a mobile user interface (UI) and user experience (UX) visualisation for smart contracts in addition to a framework for creating Ricardian contracts. The current smart contracts' contents were byte-code embedded inside the block as part of the research. The app then bound or verified the contents, producing a style sheet document. After that, data bindings and templates were automatically used to transform it to HTML or PDF so that the smart contract could be seen.

A robust incentive scheme for blockchain-based mobile crowdsensing was described by Hu et al.[66]. Their design allows for three distinct sorts of entities: miners, participants, and task initiators. Miners mine participant transactions based on predefined obligations. Public miners, on the other hand, mine the transactions that are transmitted on a public channel. As a result, every transaction is transparent and traceable. Moreover, one may contend that Hu et al.[66] do not do a sufficient job of protecting users' privacy and confidentiality during transactions.

A blockchain-based anonymous payment system with conditional anonymity enabled was proposed by Lin et al.[67] Conditional anonymity, sometimes called conditional privacy, ensures that outside observers remain anonymous even while the certifying authority (CA) has the ability to remove users' anonymity. Cybercriminals frequently use private cryptocurrencies or anonymous payment methods first (e.g., in ransomware operations). Hence, conditional anonymity and privacy are crucial for systems that protect users' and customers' privacy. The Cui et al.[68] study was very important since it incorporated the FE concept into its recommended methodology. They proposed the FE plan with the intention of outsourcing data to an unstable third-party cloud. Their primary concept is to transfer private information to the cloud, which encrypts it before sending it to the blockchain to facilitate payment processing (a procedure called decryption-based payment).

Conceptual Framework

This study uses blockchain technology to provide a secured wearable device payment system. End-to-end security for financial transactions done using blockchain technology will be provided at the application layer. Strong authentication, data integrity, secrecy, and non-repudiation security elements will all be present in the proposed payment system. The recommended strategy will prevent double- and over-spending as well as money laundering while promoting order, payment, and forward secrecy. Additionally, secure against cyberattacks, the proposed payment mechanism will be validated using blockchain technology. By addressing the various security flaws associated with mobile payments, the suggested method would let the user make purchases using a wearable device and input their private payment information for the mobile application.

Numerous wearable device-based secure authentication solutions have been introduced in the literature. However, the bulk of the solutions that are currently on the market do not include server security and instead just employ authentication techniques to link a wearable device to a mobile device. Several of the systems that are currently in use in the literature do not employ blockchain technology because of the communication and processing overheads. Due to this, the researcher has developed a safe payment system that uses blockchain technology to provide end-to-end security between users′ mobile devices, wearable technologies, payment gateways, banks, and FinTech sectors.

Because financial records are sensitive data and hence prone to attack, this project will leverage blockchain technology to protect the exchange of payment and transaction records. Because hackers or attackers may access the data so readily, security has become a top concern in the IoT. A few of the features that blockchain has built in include immutability, distributed ledgers, decentralized storage, authentication, and security. Real use cases have emerged in sectors like banking, moving past the hype. As a result, this paper would adapt Bojjagani, et al.[16] architecture for wearable devices.

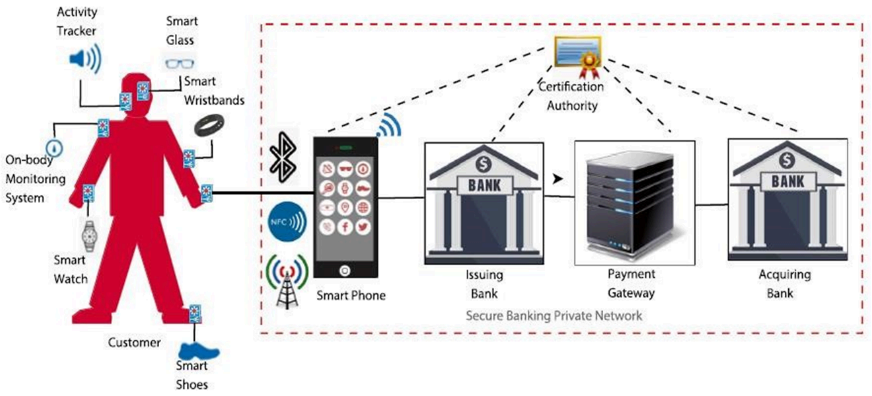

Figure 1. Architecture for wearable devices[16]

By incorporating blockchain technology into the current wearable payment system, this study seeks to propose the structure and functionality of blockchain in the context of protecting financial transactions in the banking and FinTech business. By recording how devices interact, blockchain can help to address the bulk of security flaws and traceability issues in financial transactions. Data security is increased by a blockchain since it is impenetrable and unlikely to be hacked. Blockchain technology may also eliminate trusted gatekeepers for certain apps, enabling the same programs to be operated decentralized and without a central authority. It is now possible to finish the process without sacrificing security or effectiveness, when it was previously impossible. Blockchain properties including immutability, distributed ledger, decentralisation, authentication, transparency, auditability, data encryption, and operational resilience may be used to overcome a variety of IoT architectural flaws [69].

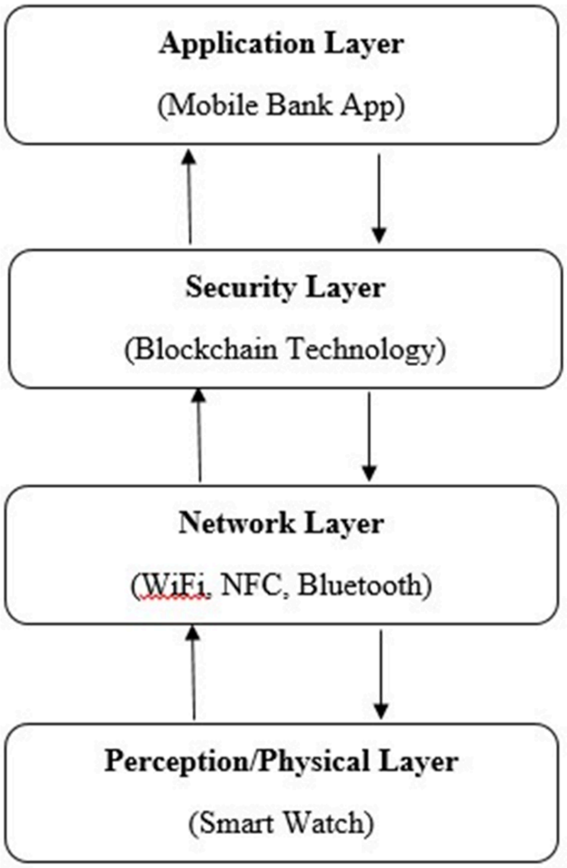

Figure 2. Proposed Wearable Device Architecture.

Every architectural layer in the proposed secure wearable financial payment system built on blockchain technology is intended to provide the best possible security and functionality. A mobile banking app will function as the user interface at the application layer, enabling smooth interactions for account management, payment processing, and transaction approvals. Real-time notifications and insights for every transaction initiated from the wearable device will be provided by this app. At the security layer, strong, unchangeable transaction records will be guaranteed through the use of blockchain technology. The immutable data storage provided by blockchain's decentralised ledger ensures that every transaction is safe, traceable, and immune to fraud.

doi.org/10.32388/K2VI7Z.2

WiFi, Bluetooth, or NFC will be used at the network layer to establish communication between the wearable device and the banking system. These technologies guarantee effective data transfer regardless of whether the wearable is utilized for contactless payments close to hand or remotely. In order to further improve security through biometric identification, the physical/perception layer will also include a wristwatch that is fitted with biometric sensors (such as fingerprint or face recognition). Advanced application, security, and network technologies work together to provide a wearable banking solution that is safe, effective, and easy to use.

Conclusion and Suggestion for Future Studies

The goal of this study is to propose a blockchain-based secure wearable payment system. Wearable technology has had a significant influence on worldwide payments, and as a result, the banking and FinTech sectors profit substantially from wearable payment systems. Therefore, the primary objective of blockchain technology is to address wearable technology's security concerns.

It is advised that the suggested secure wearable payment system based on blockchain technology be created, developed, and put into use for upcoming research to confirm its viability and efficacy. In order to do this, a working prototype that incorporates essential elements like the user interface, security measures, and networking protocols must be created. Researchers should concentrate on how usable it is in real-world circumstances to ensure that the system offers a smooth user experience while retaining a high degree of security. It is also important to assess the system's scalability, performance, and compatibility with the current payment infrastructure during the deployment phase. This would make it possible for further research to look at possible improvements, address unforeseen issues, and make sure that both financial institutions and customers can successfully use the wearable payment system.

Statements and Declarations

Author Contributions

Conceptualization: MYI, KIM, AA, YY; Methodology: MYI, KIM, AA, YY; Investigation: MYI, KIM, AA, YY; Writing – Original Draft: MYI, KIM, AA, YY; Writing – Review & Editing: MYI, KIM, AA, YY; Supervision: KIM, YY.

References

1. ^*Yilmaz NK, Hazar HB (2019). "Analysing Technology Acceptance for Internet of Things (IoT) among Accounting and Finance Students." Journal of Business Economics and Finance. **8**(4):198–208.*
2. ^*Khanboubi F, Boulmakoul A, Tabaa M (2019). "Impact of digital trends using IoT on banking processes." Procedia Computer Science. **151**:77–84.*
3. a, b, c*Abdulkader O, Bamhdi AM, Thayananthan V, Elbouraey F (2019). "IBMSDC: Intelligent Blockchain based Management System for protecting Digital Currencies Transactions." In: Third World Conference on Smart Trends in Systems Security and Sustainability. **30**:363–367.*
4. ^*Ammirato S, Sofo F, Felicetti AM, Raso C (2019a). "The potential of IoT in redesigning the bank branch protection system." Business Process Management Journal. **25**(7):1441–1473.*

5. ^Finnegan M (2020). "Banking on wearables: time for finance sector to take." Computerworld. https://www.computerworld.com/article/3556753/banking-on-wearables-time-for-finance-sector-to-take.html. Accessed 20 May 2020.
6. ^Bhutta MNM, Bhattia S, Alojail MA, Nisar K, Cao Y, Chaudhry SA, Sun Z (2022). "Towards secure IoT-based payments by extension of payment card industry data security standard (PCI DSS)." Wireless Communications and Mobile Computing. **2022**:1–10.
7. ^Malik HAM, Shah AA, Muhammad AH, Kananah A, Aslam A (2022). "Resolving Security Issues in the IoT Using Blockchain." Electronics. **11**(23):3950.
8. ^Sahoo SS, Chaurasiya VK (2023). "VIBE: blockchain-based virtual payment in IoT ecosystem: a secure decentralized marketplace." Multimedia Tools and Applications. 1–26.
9. ^Sonmez R, Sönmez FÖ, Ahmadisheykhsarmast S (2021). "Blockchain in project management: a systematic review of use cases and a design decision framework." Journal of Ambient Intelligence and Humanized Computing. 1–15.
10. ^PWC Report (2023). "Nigeria Fintech Survey." PwC. https://www.pwc.com/ng/en/publications/nigeria.
11. ^Seneviratne S, Hu Y, Nguyen T, Lan G, Khalifa S, Thilakarathna K, Hassan M, Seneviratne A (2017). "A survey of wearable devices and challenges." IEEE Commun Surv Tutorials. **19**(4):2573–2620.
12. ^Das AK, Wazid M, Kumar N, Khan MK, Choo KKR, Park Y (2017). "Design of secure and lightweight authentication protocol for wearable devices environment." IEEE J Biomed Health Inform. **22**(4):1310–1322.
13. ^Das AK, Zeadally S, Wazid M (2019). "Lightweight authentication protocols for wearable devices." Computer Electronic Engineering. **63**:196–208.
14. ^Ahamad S, Gupta P, Bikash PA, Padma KK, Khan Z, Hasan MF (2022). "The role of block chain technology and Internet of Things (IoT) to protect financial transactions in crypto currency market." Materials Today: Proceedings. **56**:2070–2074.
15. a, bAhram T, Sargolzaei A, Sargolzaei S, Daniels J, Amaba B (2017). "Blockchain technology innovations." In: IEEE Technology & Engineering Management Conference. 137–141. IEEE.
16. a, b, c, dBojjagani S, Venkateswara RPV, Vemula DR, Reddy BR, Lakshmi TJ (2022). "A secure IoT-based micro-payment protocol for wearable devices." Peer-to-Peer Networking and Applications. **15**:1163–1188.
17. ^Dachyar M, Zagloel TYM, Saragih LR (2019). "Knowledge growth and development: internet of things (IoT) research." **5**(8):2006–2018.
18. ^Bansal M, Oberoi N, Sameer M (2020). "IoT in online banking." J Ubiquitous Comput Commun Technol. **2**(4):219–222.
19. ^Mohanta BK, Jena D, Ramasubbareddy S, Daneshmand M, Gandomi AH (2021). "Addressing security and privacy issues of IoT using blockchain technology." IEEE Internet Things J. **8**(2):881–888.
20. ^Perwej Y, Ahmed M, Kerim B, Ali H (2019). "An Extended Review on Internet of Things (IoT) and its Promising Applications." Communications on Applied Electronics. **7**(26):8–22.
21. ^Kipper LM, Furstenau LB, Hoppe D, Frozza R, Iepsen S (2020). "Scopus scientific mapping production in industry 4.0 (2011–2018): a bibliometric analysis." International Journal of Production Resources. **58**(6):1605–1627.
22. ^Chen Z, Liao W, Hua K, Lu C, Yu W (2023). "Towards a synchronous federated learning for heterogeneous edge-powered internet of things." Digital Communication Network. **7**(3):317–326.

23. ^Li Y, Xia S, Cao B, Liu Q (2022). *"Lyapunov optimization-based trade-off policy for mobile cloud offloading in heterogeneous wireless networks." IEEE Trans. Cloud Comput.* ***10****(1):491–505.*
24. ^Xia S, Yao Z, Li Y, Mao S (2021). *"Online distributed offloading and computing resource management with energy harvesting for heterogeneous MEC-enabled IoT." IEEE Transactions on Wireless Communications.* ***20****(10):6743–6757.*
25. ^Silver BN, Khan M, Han K (2018). *"Internet of things: a comprehensive review of enabling technologies, architecture, and challenges." IETE Tech.Rev.* ***35****(2):205–220.*
26. ^Ben-Daya M, Hassini E, Bahroun Z (2019). *"Internet of things and supply chain management: a literature review." International Journal of Production Resources.* ***57****(15–16):4719–4742.*
27. ^Babar M, Arif F (2019). *"Real-time data processing scheme using big data analytics in internet of things based smart transportation environment." Journal of Ambient Intellectual Human Computing.* ***10****(10):4167–4177.*
28. ^Banerjee S, et al. (2019). *"A provably secure and lightweight Anonymous user authenticated session key exchange scheme for internet of things deployment." IEEE Internet of Things Journal.* ***6****(5):8739–8752.*
29. ^Abdel-Basset M, Nabeeh NA, El-Ghareeb HA, Aboelfetouh A (2020). *"Utilising neutrosophic theory to solve transition difficulties of IoT-based enterprises." Enterprise Information Systems.* ***14****(9-10):1304–1324.*
30. ^Khanna A, Kaur S (2020). *"Internet of Things (IoT), Applications and Challenges: A Comprehensive Review." Wireless Personal Communication.* ***114****:1687–1762.*
31. ^Leonardo BF, Yan-Pablo RR, Michele KS, Pedro L, Michael SD, José RL, Manuel JC, Nicola LB, Kim-Kwang RC (2023). *"Internet of things: Conceptual network structure, main challenges and future directions." Journal of Digital Communications and Networks.* ***9****(3):677–687.*
32. a, b Sultan A, Mushtaq MA, Abubakar M (2019). *"IOT security issues via blockchain: a review paper." In: Proceedings of the 2019 International Conference on Blockchain Technology. 60–65.*
33. ^Ramalingam H, Venkatesan VP (2019). *"Conceptual analysis of Internet of Things uses cases in Banking domain." In: TENCON 2019-2019 IEEE Region 10 Conference. 2034–2039.*
34. ^Ahmed-Abbasi W, Wang Z, Zhou Y, Hassan S (2019). *"Research on measurement of supply." International Journal of Distributed Sensor Networks.* ***15****(9):223–248.*
35. ^Rani SL, Susmita AM, Pranita PD (2018). *"Smart Banking Using IoT." In: International Conference on Research in Intelligent and Computing Engineering. 1–4.*
36. ^Adebayo N, Bajeh AO, Arowolo M, Udochuckwu E, Jesujana K, Ajayi M, Onyemenam J (2022). *"Blockchain Technology: A Panacea for IoT Security Challenge." EAI Endorsed Transactions on Internet of Things.* ***8****(3):225–267.*
37. ^Vemula D, Gangadharan GR (2016). *"Towards an "Internet of Things" Framework for Financial Services Sector." In: 3rd Int'l Conf. on Recent Advances in Information Technology. 978-1-4799-8579-1/16/$31.00.*
38. ^Challa S, Wazid M, Das AK, Kumar N, Reddy AG, Yoon E-J, Yoo KY (2017). *"Secure signature-based authenticated key establishment scheme for future IoT applications." IEEE Access.* ***5****:3028–3043.*
39. ^Alladi T, Chamola V, Sikdar B, Choo K-KR (2020). *"Consumer IoT: Security vulnerability case studies and solutions." IEEE Consumer Electronics Magazine.* ***9****(2):17–25.*

40. ^*Ammirato S, Sofo F, Felicetti AM, Raso C (2019b). "A methodology to support the adoption of IoT innovation and its application to the Italian bank branch security context." European Journal of Innovation Management.*
41. ^*Daniel D, Nicolas N, Ozden C, Rijkers B, Viollaz M, Winkler H (2020). "Who on Earth Can Work from Home?" The World Bank.*
42. ^*Ramos de Luna I, Montoro-Ríos F, Liébana-Cabanillas F, de Luna JG (2017). "NFC technology acceptance for mobile payments: A Brazilian perspective." Review of Business Management. **19**(63):82–103. doi:10.7819/rbgn.v0i0.2315.*
43. ^*Liébana-Cabanillas F, Ramos de Luna I, Montoro-Ríos F (2017). "Intention to use new mobile payment systems: A comparative analysis of SMS and NFC payments." Economic Research - Ekonomska Istraživanja. **30**(1):892–910.*
44. ^*Khalilzadeh J, Ozturk AB, Bilgihan A (2017). "Security-related factors in extended UTAUT model for NFC based mobile payment in the restaurant industry." Computers in Human Behaviour. **70**:460–474. doi:10.1016/j.chb.2017.01.001.*
45. ^*Liébana-Cabanillas F, Molinillo S, Ruiz-Montañez M (2019). "To use or not to use, that is the question: Analysis of the determining factors for using NFC mobile payment systems in public transportation." Technological Forecasting and Social Change. **139**:266–276.*
46. ^*Zhao H, Anong ST, Zhang L (2019). "Understanding the impact of financial incentives on NFC mobile payment adoption: An experimental analysis." International Journal of Bank Marketing. **37**(5):1296–1312. doi:10.1108/IJBM-08-2018-0229.*
47. ^*Esfahani SS, Ozturk AB (2019). "The influence of individual differences on NFC-based mobile payment adoption in the restaurant industry." J Hosp Tour Technol. **10**(2):219–232. doi:10.1108/JHTT-01-2018-0009.*
48. ^*Zhang Y, Dang Y, Brown SA, Chen H (2017). "Investigating the impacts of avatar gender, avatar age, and region theme on avatar physical activity in the virtual world." Computers in Human Behaviour. **68**:378–387. doi:10.1016/j.chb.2016.11.052.*
49. ^*Lee VH, Hew JJ, Leong LY, Tan GWH, Ooi KB (2020). "Wearable payment: A deep learning-based dual-stage SEM-ANN analysis." Expert Systems with Applications. doi:10.1016/j.eswa.2020.113477.*
50. ^*Ooi KB, Tan G (2016). "Mobile technology acceptance model: An investigation using mobile users to explore smartphone credit card." Expert Systems with Applications. **59**:33–46. doi:10.1016/j.eswa.2016.04.015.*
51. ^*Kumar D, Grover HS, Adarsh (2019). "A secure authentication protocol for wearable devices environment using ECC." Journal of Information Security and Applications. **47**:8–15.*
52. ^*Magdum A, Sivaraman E, Honnavalli PB (2021). "Contactless transaction using wearable ring with biometric fingerprint security feature." In: Computer Networks and Inventive Communication Technologies: Proceedings of Third ICCNCT 2020. 653–666.*
53. ^*Furstenau LB, Rodrigues YPR, Sott MK, Leivas P, Dohan MS, López-Robles JR, Choo KKR (2023). "Internet of things: Conceptual network structure, main challenges and future directions." Digital Communications and Networks. **9**(3):677–687.*
54. a, b*Alotaibi B (2019). "Utilizing blockchain to overcome cyber security concerns in the internet of things: A review." IEEE Sensors Journal. **19**(23):10953–10971.*
55. ^*Hang L, Kim DH (2019). "Design and implementation of an integrated IoT blockchain platform for sensing data integrity." Sensors. **19**(10):2228.*
56. ^*Dai HN, Zheng Z, Zhang Y (2019). "Blockchain for Internet of Things: A survey." IEEE Internet of Things Journal. **6**(5):8076–8094.*

57. ^*Hassan MU, Rehmani MH, Chen J (2019). "Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions." Future Generation Computer Systems. **97**:512–529.*
58. ^*Deepak P, Rajiv R, Surya N, Jinjun C (2017). "IoT and big data: An architecture with data flow and security issues." In: Cloud Infrastructures, Services, and IoT Systems for Smart Cities. 243–252. Springer.*
59. ^*Stefan KJ (2018). "A comprehensive literature review on the blockchain as a technological enabler for innovation." Dept. of Information Systems, Mannheim University, Germany. 1–29.*
60. a, b, c*Tejal S, Shalilak J (2018). "Applications of blockchain technology in banking & finance." Parul University, Vadodara, India.*
61. ^*Lawrence JT (2016). "Is disruptive blockchain technology the future of financial services?" 2016.*
62. ^*Ittay E (2017). "Blockchain technology: Transforming libertarian cryptocurrency dreams to finance and banking realities." Computer. **50**(9):38–49.*
63. ^*Fakhri D, Mutijarsa K (2018). "Secure IoT communication using blockchain technology." In: International Symposium on Electronics and Smart Devices. 1–6. IEEE.*
64. ^*White B, Kreuz T, Simons S (2019). "Midstream." In: Klaus B, Rainer K, editors. Compression Machinery for Oil and Gas. Houston, TX, USA: Gulf Professional Publishing. 387–400.*
65. ^*Jeong S, Ahn B (2022). "A study of application platform for smart contract visualization based blockchain." The Journal of Supercomputing. **78**(1):343–360.*
66. a, b*Hu J, Yang K, Wang K, Zhang K (2020). "A blockchain-based reward mechanism for mobile crowdsensing." IEEE Transactions on Computational Social Systems. **7**(1):178–191.*
67. ^*Lin C, He D, Huang X, Khan MK, Choo KKR (2020). "DCAP: A secure and efficient decentralized conditional anonymous payment system based on blockchain." IEEE Transactions on Information Forensics and Security. **15**:2440–2452.*
68. ^*Cui H, Wan Z, Wei X, Nepal S, Yi X (2020). "Pay as you decrypt: Decryption outsourcing for functional encryption using blockchain." IEEE Transactions on Information Forensics and Security. **15**:3227–3238.*
69. ^*Jain A, Yadav AK, Shrivastava Y (2019). "Modelling and optimisation of different quality characteristics in electric discharge drilling of titanium alloy sheet." Materials Today Proceedings. **21**:1680–1684.*

Declarations

Funding: No specific funding was received for this work.

Potential competing interests: No potential competing interests to declare.