Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

A Design Science Research Approach to Developing an Offline-Capable Secure Digital Wallet for Low-Connectivity Environments

Patricia Ghann

Patricia.ghann@ktu.edu.gh

Koforidua Technical University

Gabriel Teye

opanyingabbi@gmail.com

Koforidua Technical University https://orcid.org/0009-0009-5486-1344

Eric Apomah Adu

Koforidua Technical University

Isaac Junior Loveland Gavua

Koforidua Technical University

Mccarthy Newman-King

Koforidua Technical University

Carl Dela

Koforidua Technical University

Research Article

Keywords: Design Science Research, blockchain, offline digital wallets, zero-knowledge proofs, low-connectivity settings, financial inclusion, developing nations, edge computing, DAG-based ledgers, digital payments, Ghana, CBDC

Posted Date: October 7th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-11270450/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: The authors declare no competing interests.

Abstract

The rapid digitization of financial services has led to significant access disparities between underdeveloped rural areas and well-connected metropolitan centers, especially in developing countries like Ghana. Even though mobile payment systems and digital wallets are widely used worldwide, the vast majority of them require continuous internet access, rendering them ineffective in low-connectivity environments where billions of people reside. This study presents a novel artifact developed through a rigorous Design Science Research (DSR) process: the Offline-Capable Digital Wallet (OCDW). The OCDW offers a five-layer architecture that combines Directed Acyclic Graph (DAG)-based distributed ledger technology with lightweight zero-knowledge proof protocols, adaptive edge-computing authentication, and multi-channel peer-to-peer communication to enable secure, private, and efficient digital transactions in fully offline or sporadically connected environments. Unlike existing solutions that rely on expensive hardware security modules or compromise regulatory compliance for privacy, the OCDW strikes a balance through its unique tiered-trust model, which adapts security guaranties to available device capabilities while maintaining Anti-Money Laundering (AML) and Counter-Terrorism Financing (CFT) compliance through deferred synchronization mechanisms. The artifact was evaluated using functional testing, security analysis, performance benchmarking, and expert evaluation. With a transaction latency of 45 ms, a throughput of 850 transactions per second, and an energy consumption of just 12 mJ per transaction, the OCDW outperforms existing Ethereum-based and Hyperledger-based alternatives by 62% and 78%, respectively, according to the results. This paper provides a proven prototype architecture, creative design ideas for offline-capable digital wallets, and evidence-based suggestions for establishing digital payment infrastructure in developing nations. The findings have significant implications for financial inclusion strategies, central bank digital currency design, and sustainable digital payment networks in resource-constrained environments.

1.0 Introduction

The advancement of mobile devices, internet connectivity, and blockchain-based technology has drastically altered the global financial landscape during the last ten years. Once a novelty only seen in highly developed nations, digital wallets are now indispensable to daily financial transactions for billions of users worldwide. According to recent estimates, the global market for digital wallets will reach $7.5 trillion by 2027, with emerging countries having the fastest-growing categories. The vast majority of digital payment solutions are structurally dependent on continuous internet connectivity, which prevents people in remote, rural, and infrastructure-poor areas from participating in the digital economy. However, beneath this façade of progress lies a long-standing and deeply embedded divide.

The advancement of mobile devices, internet connectivity, and blockchain-based technology has drastically altered the global financial landscape during the last ten years. Once a novelty only seen in highly developed nations, digital wallets are now indispensable to daily financial transactions for billions of users worldwide. According to recent estimates, the global market for digital wallets will reach $7.5 trillion by 2027, with emerging countries having the fastest-growing categories. The vast majority of

digital payment solutions are structurally dependent on continuous internet connectivity, which prevents people in remote, rural, and infrastructure-poor areas from participating in the digital economy. However, beneath this façade of progress lies a long-standing and deeply embedded divide.

The residents of these places suffer actual economic disadvantages as a result of not having access to digital payment methods. Mobile money platforms are unable to compensate farmers for their produce when there is insufficient network coverage. Digital transactions cannot be completed by small traders during network outages. Emergency assistance payments after natural disasters are either impossible or delayed when communication infrastructure is compromised. Digital solutions are theoretically well-positioned to address the security, mobility, and traceability challenges that cash presents, even yet cash is still the most popular method of payment in these circumstances.

The issue of enabling digital payments in low-connectivity scenarios is receiving increasing attention from both central banking organizations and academic researchers. The Bank for International Settlements (BIS) has determined that offline payment capability is an essential prerequisite for Central Bank Digital Currencies (CBDCs), while the Bank of Ghana has explicitly acknowledged the need for offline-capable digital payment solutions as part of its broader financial inclusion strategy. This report attempts to close significant gaps in the body of research despite this growing awareness.

This paper presents the Offline-Capable Digital Wallet (OCDW), a comprehensive digital payment artifact designed from the bottom up to perform well in low-connectivity scenarios. Developed through a rigorous Design Science Research (DSR) methodology, the OCDW offers several innovations that differentiate it from other solutions: a distinctive five-layer architecture that separates transaction execution from real-time ledger verification; a lightweight zero-knowledge proof protocol that enables privacy-preserving transaction validation without requiring resource-intensive computations; a tiered-trust model that adjusts security guaranties to device capabilities, eliminating the need for expensive hardware security modules; and a multi-channel communication framework that enables peer-to-peer transactions via Bluetooth Low Energy, NFC, mesh networking, and SMS fallback mechanisms.

Four contributions are made by this study. It starts by describing new design ideas for offline-capable digital wallets that were created by carefully analyzing existing solutions and their drawbacks. Second, it demonstrates that safe, efficient offline digital payments are feasible without sacrificing regulatory compliance by presenting and validating a complete prototype architecture. Third, it provides empirically supported performance benchmarks that favorably contrast the proposed method with existing alternatives. Fourth, with special reference to Ghana, it offers helpful suggestions for putting in place digital payment infrastructure in developing countries that are applicable to similar contexts worldwide.

The rest of the paper is organized in this manner. Section 2 goes into great length about digital wallet technologies, offline payment systems, blockchain and distributed ledger technologies, privacy-preserving strategies, and Design Science Research methodology. It concludes with a comprehensive gap analysis. Section 3 covers the research technique, which includes the DSR framework, research questions, and design requirements. Section 4 provides a detailed description of the OCDW architecture.

Section 5 provides a detailed explanation of the offline transaction process. Section 6 reports the evaluation's findings. Section 7 discusses future work, limitations, and implications. Section 8 concludes.

2.0 Literature Review and Problem Explication

2.1 Digital Wallet Technologies

Digital wallets have evolved from simple payment credential storage systems to sophisticated platforms capable of managing a wide range of digital assets, identification credentials, and financial instruments. The core concept of a digital wallet, according to scholarly literature, consists of software-based solutions that allow users to securely store, manage, and utilize digital credentials and financial information for electronic transactions. In order to simplify online payments, the primary objectives of early implementations were to save credit card information and enable one-click checkout on e-commerce platforms.

The state of digital wallets nowadays can be divided into several groups. Custodial wallets, such as PayPal and Venmo, hold user funds and transaction data on centralized servers managed by service providers. These wallets are easy to use and convenient, but they need continuous internet access and rely significantly on the custodian. Non-custodial wallets, which are particularly popular in the cryptocurrency industry, provide users total control over their money and private keys, eliminating counterparty risk and raising user responsibility for key maintenance and security.

The emergence of Central Bank Digital Currencies has spurred a new wave of digital wallet designs focused on sovereign digital money. Zulmy et al. (2025) employed Hyperledger Fabric as the underpinning permissioned blockchain technology in their conceptual e-wallet architecture for Indonesia's Digital Rupiah. A two-tiered distribution architecture with token-based accounts secured by public-key encryption and commercial banks serving as intermediaries between the central bank and final customers was part of their concept. This architecture primarily depends on internet access for ledger synchronization and transaction validation, even if it addresses scalability and regulatory compliance challenges.

One example of how the design science approach might be applied to wallet development in a sustainable setting is the Digital Wallet for Green Travel (DWGT), which Stanivuk (2025) announced. The DWGT employs a mobile-first web application supported by blockchain infrastructure, utilizing a novel Proof of Travel Compensation (PoTC) idea implemented as a digital asset on the blockchain. The DWGT does not address offline transaction capabilities and functions in a fundamentally separate domain from financial payments in low-connectivity circumstances, despite the methodological approach being instructive.

One major flaw in the majority of digital wallet solutions is the design assumption of constant internet access. Even so-called "offline" wallets typically require sporadic internet for account synchronization, balance verification, or transaction settlement. This presumption essentially prohibits people in places

with weak connectivity from using digital financial services, even though it makes sense in urban areas with high connectivity.

2.2 Offline Payment Systems

The challenge of enabling digital payments without continuous internet connectivity has prompted a growing body of research exploring various technical approaches. Using MySQL and PHP, Shinde et al. (2023) suggested a decentralized digital offline wallet system with fast fund access. Although the system eliminates the need for payment gateway services during transactions, it relies on a centralized database architecture that has significant security flaws, including the absence of cryptographic transaction validation, susceptibility to double-spending attacks, and lack of privacy-preserving mechanisms. The alleged "99% safe" claim lacks a comprehensive security analysis, and the solution ignores the fundamental problems with offline transaction integrity.

Yoon and Kim (2025) presented a more sophisticated offline CBDC payment technique based on Trusted Platform Module (TPM) technology. Their concept employs the TPM's monotonic counter to prevent double-spending in a completely offline setting and leverages JSON Web Tokens (JWT) with digital signatures for transaction encoding. The system divides offline and online wallets, permits safe peer-to-peer connections via Bluetooth and NFC, and mandates the simultaneous usage of all valid tokens during payment processing. Despite being a significant advancement in offline payment security, this approach's practical utility is constrained by its reliance on TPM technology, which is not always available in the low-cost devices that are typical in underdeveloped countries.Furthermore, the problem of privacy-preserving compliance verification is not addressed by the protocol.

Rasheed et al. (2023) proposed a blockchain-based mobile wallet with secure offline transactions using Ethereum smart contracts and Bluetooth for direct device-to-device communication. Their solution introduces the concept of Offline Tokens (OTs), which are managed by an Offline Token Manager (OTM) smart contract, through signed token trades. The proposed solution addresses two significant drawbacks of earlier approaches: token divisibility and forgery detection. Nevertheless, cross-platform interoperability is limited by the system's reliance on Android-specific implementations, and its reliance on the Ethereum blockchain increases transaction fees and energy consumption. Because users need to maintain current public key databases locally, scalability issues are not well handled.

Rizvi and Mishra (2025) developed an offline payment system based on Time-based One-Time Password (TOTP) and SHA3-encrypted SMS to target environments with unstable internet access. By combining SMS APIs with React Native, their approach leverages telecom networks to offer offline authentication via SMS delivery channels. While this approach demonstrates creativity in utilizing pre-existing infrastructure, its dependence on telecom services causes delays and raises security issues with SIM cards. In contrast to completely autonomous offline payment systems, the system requires financial infrastructure in order to process transactions.

Fapohunda (2025) introduced an adaptive edge-computing architecture for offline digital payment authentication using Raspberry Pi 5 nodes as edge authenticators connected to mobile point-of-sale terminals via local mesh networks. The system consists of a synchronization method based on reinforcement and lightweight cryptographic handshake sequences based on elliptic curve signatures. Experimental evaluation revealed significant increases in offline authentication success rate (62% improvement) and transaction latency (43% reduction). The reliance on Raspberry Pi technology as edge nodes poses deployment and maintenance issues for wider adoption in developing regions, and the energy consumption of continuous edge node operation remains a problem.

2.3 Blockchain and Distributed Ledger Technologies

The selection of an appropriate distributed ledger technology, which has significant implications for scalability, energy efficiency, security, and adaptation for environments with limited resources, is crucial to the design of any blockchain-based digital wallet. Conventional blockchain implementations, like Ethereum and Bitcoin, rely on sequential block chaining and proof-of-work or proof-of-stake consensus techniques, which have high computational and energy requirements. These characteristics make first and second-generation blockchains unsuitable for usage in developing countries with expensive electricity and limited device capabilities.

Pradhan et al. (2022) investigated the IOTA Tangle as a lightweight alternative to peer-to-peer energy trading, highlighting its advantages in terms of low confirmation latency, high throughput, and zero transaction fees. The Tangle's Directed Acyclic Graph (DAG) structure makes concurrent transaction validation possible and does away with the need for miners—features that are particularly relevant for low-value, high-volume payment scenarios that are typical in poor countries. In terms of confirmation latency and throughput metrics, IOTA outperforms Ethereum and Hyperledger Fabric, particularly for bundle sizes of five and ten transactions, according to their benchmarking results. However, the IOTA implementation also highlighted problems with address reuse security and the complexity of Masked Authentication Messaging (MAM) channel management.

Zulmy et al. (2025) selected Hyperledger Fabric for their e-wallet concept because to its permissioned access method, adaptable design, and suitability for enterprise applications. Although Hyperledger Fabric offers robust access control and privacy protections through channel-based isolation, its ordering service architecture adds latency that is problematic for real-time payment applications and its resource requirements are higher than those of low-end mobile devices. Additionally, the platform's complexity makes deployment challenging in environments with limited technological expertise.

Seidemann et al. (2026) used the BIS methodology to assess the technical viability of offline-capable CBDCs as crucial enablers of reliable digital payment systems. Their investigation, which contrasted token-based designs with traditional account-based systems, found that token-based CBDCs can preserve the two-tier distribution model known from the cash cycle while allowing offline transactions through bearer instrument characteristics. Their layered security architecture, which includes hardware security, robust payment protocols, and the central bank's ability to prevent double-spending, provides a

helpful basis for thinking about offline payment security, even though the exact implementation still depends on hardware security modules.

Atangana et al. (2026) provided a comprehensive systematization of data on offline-capable digital currency protocols by analyzing the security features, architectural choices, and deployment issues of existing approaches. Their taxonomy distinguishes three fundamental approaches to offline capability: hardware-assisted security (using secure elements or TPMs), cryptographic proof systems (using zero-knowledge proofs or blind signatures), and trusted execution environments (using TEE capabilities). The systematization demonstrates that no existing solution adequately addresses the intersection of offline capability, minimal resource requirements, privacy preservation, and regulatory compliance.

2.4 Zero-Knowledge Proofs and Privacy-Preserving Mechanisms

Zero-knowledge proofs (ZKPs) are currently a crucial cryptographic basic for achieving privacy-preserving verification in digital payment systems. A zero-knowledge proof allows one party (the prover) to demonstrate to another (the verifier) that a specific claim is true without revealing any information other than the statement's veracity. In the context of offline digital payments, ZKPs allow a payer to show that they have sufficient funds and that a transaction meets regulatory criteria without revealing their identity, account balance, or transaction history.

Mondal and Chithralekha (2025) introduced an offline CBDC model for IoT scenarios that protects privacy by integrating secure elements with intermittent synchronization and zero-knowledge proofs. Their approach employs a hierarchical wallet structure, with a core wallet on mobile devices and sub-wallets with Secure Elements (SEs) on IoT devices. The system uses Zero-Knowledge Proofs to confirm that transactions satisfy four crucial criteria: possession of relevant funds, transfer value validity, AML/CFT limitation compliance, and credential irrevocability. The payee's local ZKP verification enables transaction execution without internet access. However, the system's accessibility is limited by its dependency on secure element hardware, and the computational demands of ZKP generation on IoT devices with limited resources remain a worry.

The tension between privacy and regulatory compliance is one of the main challenges of offline digital payment systems. Traditional compliance techniques depend on real-time transaction monitoring and identity verification, both of which are practically unachievable in offline environments. This contradiction is resolved by Yoon and Kim's (2025) ID certificate solution, in which each offline CBDC wallet has a public key pair inside the TPM and is protected by an ID certificate from the CBDC institution. The certificate contains an identifier for the wallet in place of the subscriber's actual name, enabling administrative oversight and a certain degree of pseudonymity. However, this approach still requires TPM hardware and can not provide the strong anonymity guaranties that ZKP-based approaches can.

When selecting appropriate ZKP protocols for resource-constrained applications, there are important trade-offs between proof size, generation time, verification time, and security assumptions. Succinct

non-interactive arguments of knowledge (zk-SNARKs) offer small proof sizes and fast verification, but they require a dependable setup. Despite producing larger proofs, zk-STARKs eliminate the need for trustworthy setup. Bulletproofs offer appropriate proof sizes without a trusted setup, but their verification costs are higher. When assessing these trade-offs for the OCDW, the target deployment environment—where devices may have limited processing power, memory, and battery capacity—must be taken into account.

2.5 Design Science Research in Information Systems

Design Science Research (DSR) has established itself as a rigorous approach to creating and evaluating innovative information systems artifacts. Hevner et al. (2004) state that DSR comprises creating new artifacts to address concerns that have been identified and then assessing those artifacts to demonstrate their usefulness and efficacy. The methodology distinguishes itself from natural science research by focusing on "how things can be" rather than "how things are," and it is particularly well-suited for developing novel technical solutions to practical problems.

A number of crucial tasks make up the DSR methodology, such as problem identification and motivation, defining objectives for a solution, designing and developing the artifact, demonstrating the artifact in a relevant context, evaluating the artifact against objectives, and communicating the results to the appropriate audiences. Because DSR is iterative, it ensures that the final product is both innovative and beneficial by allowing the artifact to be progressively enhanced depending on evaluation input.

By using the DSR technique to create the Digital Wallet for Green Travel, Stanivuk (2025) showed how it may be operationalized in the field of digital wallets. The development and improvement of requirements were greatly aided by stakeholder interviews and iterative feedback, and the study moved methodically from problem inquiry through treatment design and evaluation to artifact execution. The methodological rigor of this work provides a model for applying DSR to the development of offline-capable digital wallets.

There are several benefits of using DSR in digital wallet development when compared to purely technological or conceptual methods. By basing artifact design on in-depth problem research and stakeholder participation, DSR ensures that the final solution satisfies real user needs rather than theoretical ones. The DSR assessment component provides evidence of artifact utility, which is essential for both scholarly contribution and practical implementation. The iterative structure of the methodology accommodates the uncertainty and complexity associated with developing new technologies for challenging deployment scenarios.

2.6 Research Gap Analysis

The investigation presented in this paper is motivated by many important gaps found in the body of current knowledge. These gaps present opportunities to significantly impact the intersection of digital wallet technologies, physical payment capabilities, and financial inclusion in emerging countries.

Gap 1

The first gap is the lack of thorough DSR-based methods. None of the several papers that have proposed technical solutions for offline digital payments have employed a rigorous Design Science Research process that systematically proceeds from problem explanation through iterative design, evaluation, and improvement. The absence of such methodological rigor limits the validity and generalizability of existing contributions.

Gap 2

Hardware dependence of security models. Strong security guaranties provided by existing offline payment systems, like those proposed by Mondal and Chithralekha (2025) and Yoon and Kim (2025), rely on specialized hardware (TPMs, Secure Elements) that is not available in the low-cost devices typical of developing countries. Security and privacy are compromised by commodity hardware-based solutions, creating a challenging trade-off that limits accessibility.

Gap 3

Inefficient energy utilization. Blockchain-based solutions, particularly those based on Ethereum or Hyperledger Fabric, impose energy costs that are unsustainable in developing countries where devices with small battery capacities and uncertain power availability are common. The energy consumption of proof-of-work consensus, ongoing network synchronization, and smart contract execution is a significant barrier to adoption.

Gap 4

Unresolved tension between compliance and privacy. No existing solution adequately addresses the tension between user privacy and legal compliance in offline settings. While compliance-maintaining solutions typically compromise privacy through identity linking, strong privacy solutions compromise AML/CFT compliance and auditability.

Gap 5

Limited attention on developing areas. Most of the existing research on offline digital payments is conducted in resource-rich lab environments, making assumptions about device capabilities, network availability, and user technical literacy that do not truly reflect conditions in developing countries. The particular problems of rural Ghana and other environments, like limited digital literacy, intermittent energy, low smartphone adoption, and regulatory constraints, are not given enough attention.

Gap 6

Insufficient compatibility. Existing systems, which often focus on a single communication channel or device type, lack the multi-channel flexibility needed to handle different usage situations and device capabilities in developing regions.

Table 1
Summary of Research Gaps and OCDW Contributions

Gap	Description	OCDW Contribution
Methodological	No rigorous DSR approach to offline wallet	Complete DSR lifecycle with stakeholder engagement
Hardware Dependency	Reliance on TPM/SE not available in low-cost devices	Tiered-trust model adapting to device capabilities
Energy Efficiency	High energy consumption of existing blockchain solutions	DAG-based ledger with 78% lower energy consumption
Privacy-Compliance	Unsolved tension between anonymity and AML/CFT verification	Lightweight ZKP with deferred compliance
Regional Focus	Limited attention to developing region constraints	Designed specifically for low-connectivity environments
Interoperability	Single-channel, single-device limitations	Multi-channel BLE/NFC/Mesh/SMS support

3.0 Research Methodology

3.1 Design Science Research Framework

Design Science Research (DSR), which follows the guidelines established by Hevner et al. (2004) and the enhanced DSR cycles framework published by Peffers et al. (2007), is the primary methodological framework used in this study. The DSR approach is particularly appropriate for this study because it focuses on the creation of a new artifact (the OCDW) that addresses a clearly defined problem (the lack of secure digital payment access in low-connectivity environments) and provides methods for a comprehensive evaluation of the artifact's utility and efficacy.

The research methodology, which iterates toward the final artifact, consists of five interconnected cycles: the Relevance Cycle, which ensures that the research addresses a real problem of interest to practitioners; the Rigor Cycle, which guaranties methodological soundness and grounds the research in existing knowledge; the Design Cycle, which includes the iterative construction and evaluation of the artifact; the Evaluation Cycle, which methodically evaluates the artifact against predetermined criteria; and the Communication Cycle, which disseminates findings to relevant stakeholders.

The Relevance Cycle was initiated through stakeholder interviews with financial inclusion practitioners, central bank officials, and leaders of Ghanaian rural communities. These exchanges highlighted the significance of the offline payment problem and clarified the specific requirements and constraints that any practical solution must satisfy. Section 2 of this study states that a comprehensive literature review including blockchain topologies, digital wallet technologies, offline payment protocols, and privacy-preserving strategies was part of the Rigor Cycle.

As part of the Design Cycle, requirements formulation, architectural design, prototype implementation, and formative evaluation were all carried out repeatedly. With each iteration, the artifact's functionality, performance, and usability were progressively enhanced by incorporating feedback from the previous evaluation. In the first major design iteration, the core architectural foundation was built; in the second, security and privacy methods were improved; and in the third, performance was optimized for low-resource devices.

Design Science Research Methodology for OCDW Development

3.2 Research Questions

The following research questions guide the investigation and provide structure for evaluating the research contributions:

RQ1

Which architectural concepts ought to direct the creation of a digital wallet that can carry out safe transactions in settings with sporadic or non-existent internet connectivity?

RQ2

How can transaction validation that protects privacy be accomplished in offline settings without the need for pricey hardware security modules while yet adhering to anti-money laundering and counterterrorism financing laws?

RQ3

What performance attributes can be attained by an offline-capable digital wallet intended for use on inexpensive mobile devices in developing nations, and how do these contrast with those of current solutions?

RQ4

What useful recommendations come out of the design and assessment process that can guide the implementation of digital payment infrastructure in comparable low-connectivity settings around the world?

3.3 Problem Identification and Justification

This study aims to solve the issue of current digital payment systems' inability to support populations in low-connectivity situations, which results in financial exclusion and perpetuates economic inequality. There are several reasons why this matter is significant. First, the magnitude of the affected population is demonstrated by the fact that over one-third of the world's population lacks reliable internet connectivity. Second, by limiting access to markets, government services, credit, and insurance, financial

exclusion has a detrimental effect on the economy. Third, infrastructure problems in remote and rural areas are not expected to be resolved in the near to medium term due to budgetary and geographic constraints, making the problem persistent.

The issue is also intellectually challenging, requiring original solutions at the intersection of distributed systems, human-computer interaction, cryptography, and regulatory compliance. Merely adding periodic synchronization to current online payment systems is insufficient because it leads to security vulnerabilities (particularly with regard to double-spending), privacy risks (because of transaction pattern analysis), and usability problems (because of complex synchronization procedures). It necessitates a whole new architectural approach.

3.4 Design Requirements and Constraints

The design of the OCDW is governed by a comprehensive set of requirements derived from stakeholder input, literature analysis, and contextual constraints. These needs are classified into functional, non-functional, and constraint categories.

functional requirements. Bluetooth Low Energy, NFC, Wi-Fi Direct, mesh networking, SMS fallback, token generation and management capabilities for offline value representation, cryptographic transaction signing and validation, deferred synchronization with the central ledger when connectivity becomes available, multi-device wallet operation with consistent state, and transaction history and balance inquiry capabilities in offline mode are just a few of the communication channels that the OCDW must support.

Non-functional requirements. The OCDW must operate on Android devices with quad-core processors and 2GB RAM, achieve transaction latency of less than 100 ms, maintain network throughput of at least 500 transactions per second, use no more than 20 mJ of energy per transaction on target devices, provide user-friendly interfaces that are accessible to people with low levels of digital literacy, support English and major local languages like Twi, Ga, and Ewe, and maintain backward compatibility with the current mobile money infrastructure.

Requirements for privacy and security. Without real-time ledger access, the OCDW must prevent double-spending; guarantee transaction non-repudiation through cryptographic signatures; safeguard user privacy through zero-knowledge balance proofs; fend off token forgery and replay attacks; support regulatory compliance through deferred audit trail generation; implement secure key storage using available device capabilities; and offer graceful degradation of security guarantees based on device capabilities.

Restrictions imposed by laws. In addition to implementing know-your-customer (KYC) identity verification, supporting transaction amount limits as required by regulations, facilitating the reporting of suspicious activity through deferred synchronization, maintaining unchangeable audit trails for regulatory review, and working with the current financial system infrastructure, the OCDW must comply with the Bank of Ghana's digital payment regulations.

4.0 Artifact Design: The OCDW Architecture

4.1 Architectural Overview

The Offline-Capable Digital Wallet us (OCDW) five-layer architecture allows for secure offline operation while maintaining consistency with the global ledger state upon synchronization by separating transaction execution from real-time ledger verification. The architecture is based on the progressive trust principle, which enables security guaranties to adapt to current device capabilities and communication scenarios rather than requiring a predetermined hardware baseline. This approach ensures that the OCDW can operate effectively on a wide range of devices found in underdeveloped countries, from basic cellphones to more advanced versions, without compromising crucial security aspects.

Five layers make up the OCDW architecture: the Presentation Layer, which provides user-facing interfaces; the Application Layer, which handles transaction management and core wallet logic; the Security and Trust Layer, which provides cryptographic services and builds trust; the Blockchain and Consensus Layer, which maintains distributed ledger state and transaction ordering; and the Communication Layer, which enables peer-to-peer data exchange via multiple channels. As technology advances, components can independently change and be replaced since each layer has unique interfaces and functions.

For the proposed use case, the OCDW design offers significant advantages over traditional blockchain topologies since it integrates a distributed ledger based on DAG at the consensus layer. The DAG structure enables parallel transaction validation, eliminates miner fees, and boosts throughput while consuming less energy. These characteristics are essential for sustainable operation in developing countries, because energy efficiency directly affects adoption and usefulness.

Proposed OCDW System Architecture

4.2 Presentation Layer

The Presentation Layer, which was developed with careful attention for the needs of populations with varying degrees of digital literacy and device capabilities, provides the interface between users and the OCDW system. The four primary interface components of the layer are the Mobile Wallet Application, which provides a fully functional interface for smartphones; the USSD Interface, which uses unstructured supplementary service data codes to enable basic functionality on feature phones; the Agent Interface, which enables intermediary-assisted transactions for users without direct device access; and the Administrative Dashboard, which provides system operators with monitoring and management capabilities.

The Mobile Wallet Application is designed as a Progressive Web Application (PWA) to reduce storage requirements and enable operation across a range of device kinds. In keeping with the principles of progressive disclosure, the interface design simplifies basic tasks (such sending, receiving, and

checking balances) while providing expert users with access to complex features. Every interface element is designed to be readable in outdoor lighting conditions typical of rural market situations, with wide touch targets and high contrast color schemes. Voice-guided operation for critical functions can be beneficial for users with low reading skills.

Thanks to the USSD Interface, OCDW is now accessible to many feature phone customers in rural Ghana. Through a structured menu system accessible with standard GSM codes, users may initiate token requests, check balances, and validate transactions using simple numerical inputs. Despite their inherent security limitations (since feature phones lack cryptographic capability), USSD-based transactions are integrated into the tiered-trust paradigm as a low-assurance channel appropriate for small-value transactions.

4.3 Application Layer

In addition to managing transaction lifecycles, coordinating interactions between other architectural levels, and enforcing business rules, the Application Layer implements the core business logic of the OCDW. The five main components of the layer are: the Compliance Engine, which enforces regulatory constraints like transaction limits and reporting requirements; the Transaction Manager, which coordinates the entire transaction process; the Offline Validator, which validates transactions locally without access to the ledger; the Identity Service, which manages user identity credentials and KYC verification; and the Sync Manager, which oversees deferred synchronization with the central ledger.

The Transaction Manager uses a state machine model for transaction processing, with defined states for initiation, validation, execution, confirmation, and completion. Each transaction progresses through these phases based on device capabilities, counterparty responses, and network availability. The state machine design makes it easy to recover from disruptions and provide customers with clear feedback because transactions are always in a well-defined state.

The Offline Validator, which assesses whether a particular transaction can be completed without real-time ledger access, is one of the OCDW's primary innovations. The validator uses a variety of heuristics and cryptographic tests, including verifying the validity of the payer's token, assessing the token's provenance and freshness, and comparing the transaction amount to previous spending patterns, to ascertain the probability of double-spending. Although offline validation cannot provide the same guaranties as online ledger verification, the validator's risk assessment directs the deployment of appropriate security measures, such as requiring additional authentication for higher-risk transactions.

The Compliance Engine encodes regulatory requirements as configurable rules that are enforced both offline (via local constraint checking) and during synchronization (through comprehensive audit and reporting). The engine provides threshold-based reporting, velocity checks, and transaction amount restrictions, allowing it to adapt to evolving regulatory requirements without requiring client-side modifications.

4.4 Security and Trust Layer

The Security and Trust Layer, which uses a tiered-trust paradigm that adjusts security measures based on device capabilities, provides the cryptographic foundations of OCDW security. The layer consists of five components: the HSM/TEE Interface, which provides access to hardware security features when available; the Fraud Detector, which employs behavioral analysis to identify suspicious activity; the Lightweight ZKP Module, which generates and validates zero-knowledge proofs of solvency and compliance; the Key Management Service, which oversees the generation, storage, and rotation of cryptographic keys; and the Audit Logger, which maintains tamper-evident records of security-relevant events.

The Lightweight ZKP Module, one of the OCDW's key achievements, was developed to overcome the computational limitations that have prevented zero-knowledge proofs from being implemented on low-resource devices. The module implements an improved version of the Bulletproofs protocol specifically for range proofs on transaction amounts. Through careful algorithm selection, parameter optimization, and implementation-level improvements such as concurrent proof production and precomputation of common parameters, the module achieves proof generation times < 30 ms on target devices with proof sizes of approximately 672 bytes. This is a significant improvement over generic implementations, which compute on similar hardware in a matter of seconds.

The tiered-trust approach creates three levels of trust based on the device's capabilities. Trust Level 1 (Basic) covers devices without hardware security features that rely on software-based key storage and standard cryptographic processes. Trust Level 2 (Enhanced) allows hardware-isolated key storage and attestation for devices that support the Trusted Execution Environment (TEE). The strongest security guaranties are provided by Trust Level 3 (Maximum), which applies to devices with specific Hardware Security Modules (HSMs) or Secure Elements (SEs). The trust level determines the transaction restrictions, authentication requirements, and synchronization frequency applied to each wallet in order to guaranty that security measures are proportionate to available protections.

Multi-Layer Security Framework for OCDW

4.5 Blockchain and Consensus Layer

The Blockchain and Consensus Layer sustain the distributed ledger state that underpins the OCDW's security paradigm. The OCDW employs a DAG-based ledger topology that was influenced by IOTA's Tangle, in contrast to traditional blockchain implementations. For the target deployment context, this ledger structure offers several advantages, such as: lower energy consumption because the DAG structure does not require energy-intensive mining or staking; parallel transaction validation, which offers higher throughput than sequential block-based approaches; elimination of transaction fees, which permits economically feasible micro-transactions; and suitability for lightweight clients because transaction participation does not require full node operation.

For each new transaction to be accepted in the directed acyclic graph of transactions that the DAG implementation maintains, two previous transactions must be validated. This validation-by-transaction

approach creates a self-reinforcing framework where transaction confirmation confidence increases with time since subsequent transactions indirectly validate earlier ones. The OCDW adapts this model for offline operation through a two-phase validation process: local validation during peer-to-peer exchange, where parties verify each other's tokens using cached ledger state, and global validation during synchronization, where offline transactions are integrated into the DAG and their confirmation confidence is established.

The Offline Token Manager (OTM), a specialized component, issues, tracks, and redeems offline tokens that represent value during disconnected operation. When a user transitions from online to offline mode, the OTM converts a portion of their on-ledger balance into cryptographically signed tokens of predetermined denominations. These tokens can be exchanged with other OCDW users over the offline transaction protocol and redeemed for on-ledger credit once connectivity is restored. The OTM uses a serial number tracking technique to prevent token duplication and make double-spending detection easier during synchronization.

The rules governing token issuance, redemption, and compliance verification are included in the smart contracts of the OCDW ledger. Because these contracts are designed in a domain-specific language suited for the limited computational capabilities of the intended deployment environment, they offer essential functionality without the overhead of general-purpose smart contract platforms like Ethereum.

4.6 Communication Layer

The Communication Layer provides robustness against the loss of any one communication mechanism, enabling peer-to-peer data exchange over several channels across OCDW instances. Wi-Fi Direct, which supports higher-bandwidth peer-to-peer connections for batch transactions or multi-party exchanges; Bluetooth Low Energy (BLE), which provides low-power, short-range communication suitable for face-to-face transactions; Near Field Communication (NFC), which enables tap-to-pay transactions between adjacent devices; Mesh Networking, which increases transaction range by routing through intermediary devices; and SMS/GSM Fallback, which enables basic transaction functionality through cellular text messaging in the event that data connectivity is unavailable.

The multi-channel approach ensures that transactions can be completed in a range of scenarios: rural traders can exchange value through BLE at distances up to 100 meters; market vendors can accept payments via NFC tap; community agents can process batch transactions through Wi-Fi Direct; and even users with only basic feature phones can participate through SMS-based token exchange. The Communication Layer intelligently selects the optimal channel based on availability, range requirements, and security considerations with seamless channel changeover during active sessions.

5.0 Offline Transaction Protocol

5.1 Protocol Phases

Through four distinct stages, the OCDW offline transaction protocol guaranties safe value exchange between parties without requiring real-time ledger access. The protocol ensures non-repudiation, prevents double-spending, and protects privacy while enabling efficient execution on low-resource devices.

Phase 1

Token Request and Verification. The sender initiates a transaction by giving the recipient their offline tokens and a zero-knowledge verification of the tokens' legitimacy and the sender's sufficient balance. The recipient uses parameters preserved from their most recent synchronization with the ledger to verify the proof that the tokens have authentic signatures from the token issuance authority and have not been recorded as spent.

Phase 2: ZKP Development and Verification. Three characteristics are attested to by the sender's lightweight zero-knowledge proof: (a) the transaction complies with applicable regulatory limits; (b) the tokens have not been spent since the sender's last synchronization, as verified by a freshness counter; and (c) the sender has valid tokens with a total value at least equal to the transaction amount. After the evidence is locally created using the best Bulletproofs parameters, the receiver checks it in around 15 milliseconds.

Phase 3

Tokens being exchanged between peers. Once proof verification is complete, the parties engage in a cryptographic token exchange procedure. The sender transfers ownership of tokens worth the transaction amount to the recipient by signing the transfer with their private key. The recipient produces a signed acceptance of receipt as proof of payment. Both parties update token inventories and local transaction records. In the sender's local state, the transferred tokens are marked as spent and added to the recipient's token collection.

Phase 4

Verifying and documenting. The transaction is submitted to the central ledger and recorded in both parties' local tamper-evident audit logs during the subsequent synchronization. The transaction appears to be finished from the user's perspective, but ledger integration is required for final settlement.

Offline Transaction Protocol Flow

5.2 Lightweight ZKP Implementation

The OCDW's zero-knowledge proof system is a significant breakthrough that enables privacy-preserving transaction validation without the computational cost of general-purpose ZKP protocols. The method builds upon the Bulletproofs range proof structure with certain optimizations designed specifically for the offline payment environment.

The fundamental demonstration demonstrates that a committed value is within a valid range (0 to maximum transaction amount) without revealing the actual value. This is achieved by employing an inner product argument to reduce the range proof to a logarithmic-size statement. The OCDW implementation optimizes this architecture by precomputing generating points, analyzing inner product rounds in parallel using SIMD instructions on target devices, and aggressively truncating proof sections when security analysis permits.

The resulting proof is around 672 bytes in size and can be generated in 28 milliseconds on a quad-core ARM CPU operating at 1.4GHz. Since verification takes around 15 ms, the ZKP overhead is negligible in comparison to the communication latency for typical peer-to-peer transactions. These performance numbers show a significant improvement over typical Bulletproofs implementations, which need several hundred milliseconds for proof production on equivalent hardware.

The ZKP module employs a composite proof in addition to range proofs that demonstrates solvency (total available funds exceed transaction amount), freshness (tokens were acquired after the prior reported synchronization), and compliance (transaction amount is within regulatory constraints). The composite proof is more effective than developing separate proofs for each property since shared randomness and commitment structures reduce the overall proof size and generation time.

5.3 Token Lifecycle Management

The carefully controlled lifespan of offline tokens in the OCDW guaranties value consistency across the on-ledger and off-ledger states. The lifecycle consists of five stages: issuance, activation, circulation, redemption, and retirement.

Issuance: When a user requests offline capabilities, the OTM generates a set of tokens that represent a predefined percentage of their on-ledger balance. Each token has a unique serial number, denomination, issuance and expiration dates, and an OTM digital signature. Tokens are given in predetermined denominations (e.g., 1, 5, 10, 20, and 50 units) to allow precise payment without requiring the capacity to create change.

Activation

Issued tokens become active when the user's device synchronizes with the OTM. The ledger state is modified to reflect that the related balance is now being held offline after the token signatures are downloaded. Activation establishes the start of the token's validity term and records the identity of the issuing device for tracing purposes.

Circulation

OCDW users can exchange activated tokens through the offline transaction protocol. Each trade affects token ownership by cryptographic transfer, and the complete chain of ownership is recorded in the

token's information. This provenance chain enables the detection of attempts at double spending during synchronization.

Redemption

When a user synchronizes with the ledger, their accrued tokens are converted into on-ledger credit. Before crediting the user's on-ledger balance, the OTM verifies the legitimacy of each token and checks for double-spending against the global token registry. Tokens that have been reported as spent or that have expired are not accepted.

Retirement

Tokens that have been successfully redeemed are marked as retired in the global registry and are no longer available for circulation. Since retirement is permanent and irreversible, tokens cannot be redeemed.

5.4 Deferred Synchronization

Deferred synchronization is the process of incorporating offline transactions into the global ledger state and ensuring eventual consistency between off-ledger and on-ledger value representations. The synchronization process is designed to work well across intermittent, low-bandwidth connections, which are typical in developing countries.

As soon as a device joins, the Sync Manager initiates a synchronization session with the nearest gateway node. The session begins with a brief state overview that enumerates the offline transactions that are still awaiting integration. The gateway node checks for double-spending, regulatory compliance, and cryptographic integrity by comparing these transactions to the current ledger state. Valid transactions are included into the DAG, whereas questionable or invalid transactions are flagged for manual review.

The synchronization protocol makes advantage of several enhancements to save bandwidth and energy consumption. Transaction batches are compressed using delta encoding so that only the modifications from the previously synchronized state are sent. Conflict resolution follows the last-writer-wins rule for benign conflicts (such as parallel balance adjustments on the same account); it starts escalation for malicious disputes (such as attempts at double spending). By including high-priority transactions first and postponing less significant updates, progressive synchronization enables devices with intermittent connectivity to submit transactions gradually.

The role of deferred synchronization in regulatory compliance is an essential element. During synchronization, the Compliance Engine generates the data required by AML/CFT regulations, such as aggregate data, suspicious activity indications, and transaction records beyond predefined criteria. By submitting these reports to the regulatory authority through the gateway node, they fulfilll compliance obligations that cannot be met during offline operation.

6.0 Evaluation

6.1 Evaluation Strategy

In order to assess the OCDW artifact's efficacy, quality, and usefulness in a variety of contexts, a multimodal method is used. Four complementary techniques make up the evaluation framework: expert review, which gathers qualitative feedback from potential users and domain experts; performance benchmarking, which compares the operational characteristics of the system to competing solutions and specified requirements; security analysis, which assesses the system's resistance to known attack vectors; and functional testing, which verifies that the system functions as intended.

The evaluation was conducted using three rounds of the design cycle, each of which improved the artifact based on the findings of the previous evaluation. The primary objective of the first iteration was to validate the basic architecture concepts and transaction functionality. In the second iteration, the privacy guaranties and security mechanisms were assessed in an adversarial environment. Usability and performance characteristics were evaluated in a deployment environment simulation during the third iteration.

6.2 Functional Testing Results

Functional testing was conducted using a comprehensive test suite of 147 distinct test cases that covered the system's functional components. The tests were conducted using a representative variety of devices, including entry-level Android smartphones (2GB RAM, quad-core 1.4GHz processor), mid-range devices (4GB RAM, octa-core 2.0GHz processor), and a Raspberry Pi 4 as an edge node simulator.

Table 2
Functional Testing Results Summary

Component	Test Cases	Passed	Failed	Pass Rate
Transaction Manager	35	35	0	100%
Offline Validator	28	27	1	96.4%
ZKP Module	24	24	0	100%
Token Manager	22	22	0	100%
Sync Manager	20	19	1	95.0%
Communication Layer	18	18	0	100%
Total	147	145	2	98.6%

The two unsuccessful test cases concerned edge situations in the Sync Manager (recovery from gateway node disconnection while active synchronization) and the Offline Validator (managing malformed tokens from corrupted devices). In later rounds, these problems were fixed via better session state management and input validation.

6.3 Security Analysis

The security analysis process included formal protocol verification, penetration testing, and threat modeling. Resistance to man-in-the-middle attacks, non-repudiation, privacy preservation, resistance to token forging, and prevention of double-spending were the five key security features that were the focus of the inquiry.

avoiding overspending. The OCDW employs a multi-layered approach that combines local validation, token serial number tracking, and global conflict detection to prevent double-spending. Formal proof utilizing the Tamarin protocol prover shows that the protocol prevents double-spending under the Dolev-Yao attacker model when at least one honest actor is involved. Practical testing revealed 100% detection of double-spending attempts during synchronization with a mean detection latency of 2.3 seconds.

opposition to token forgeries. Tokens are safeguarded by digital signatures from the OTM, making forgery computationally unfeasible without access to the OTM's private key. The signature system provides 128-bit security using the secp256k1 curve and ECDSA. The most widely used techniques would require roughly 2^{128} computations to try forgery assaults, which is far more than the existing CPU capacity.

privacy protection. The ZKP-based balance verification ensures that the parties only learn about the validity of the transaction, not the actual balances or transaction histories of their counterparts. Analysis confirmed the proof system's entire zero-knowledge features, which state that the verifier learns nothing other than the validity of the assertion being proven.

non-repudiation. Every transaction is cryptographically signed by both parties, providing unquestionable evidence of participation. The signature system satisfies the existential unforgeability under chosen message attack (EUF-CMA) security definition.

Table 3
Security Analysis Results

Security Property	Mechanism	Verification Method	Result
Double-spending prevention	Serial tracking + ZKP freshness	Tamarin prover + penetration test	Satisfied
Token forgery resistance	ECDSA signatures	Cryptographic analysis	128-bit security
Privacy preservation	Optimized Bulletproofs	Zero-knowledge proof	Perfect ZK
Non-repudiation	Dual-party signatures	EUF-CMA analysis	Satisfied
MITM resistance	Authenticated key exchange	Protocol analysis	Satisfied
Replay protection	Freshness counters	Penetration test	100% detection

6.4 Performance Benchmarking

For performance benchmarking, standardized hardware representative of the anticipated deployment environment was utilized. A Xiaomi Redmi 9A (2GB RAM, MediaTek Helio G25 octa-core 2.0GHz) was introduced for cross-device comparison, however the Samsung Galaxy A03 (2GB RAM, Unisoc SC9863A octa-core 1.6GHz) was the primary test device in the test environment. Each test was carried out using fully charged batteries in a controlled environment at 25 degrees Celsius.

With a transaction latency of 45 ms for peer-to-peer exchanges, the OCDW satisfied the sub-100 ms operation requirements. The remaining time is spent on state updates and logging; the majority of this latency is caused by communication setup time (18 ms for BLE pairing), ZKP verification (15 ms), and signature validation (8 ms). Throughput tests show that the system can handle 850 transactions per second at the network level, which is significantly more than the necessary 500 TPS.

Energy usage was measured using a Monsoon Solutions Power Monitor that was connected to the test device's battery connections. With an average of 12mJ per operation, the OCDW was well within the 20mJ limit. This performance is due to the enhanced ZKP implementation, the efficient BLE communication protocol, and the lightweight DAG-based consensus method. A basic Ethereum-based solution utilized 54mJ per transaction on the same hardware, which is 78% less energy.

Performance Benchmarking Results

6.5 Comparative Analysis

In six dimensions, offline capability, blockchain type, hardware dependency, privacy mechanism, adoption of DSR approach, and developing area focus the OCDW was contrasted with nine current offline or hybrid digital wallet systems.

Comparative Analysis of Offline Digital Wallet Solutions

According to the comparative analysis, the OCDW is the only system that simultaneously provides full offline capability, cheap hardware requirements, stringent DSR technique, privacy-preserving ZKP approaches, and explicit developing region focus. Even if some of the current solutions are great, they do not fully satisfy the requirements for successful implementation in underdeveloped areas with poor connectivity.

Table 4
Quantitative Performance Comparison

Metric	OCDW (Proposed)	Rasheed et al.	Yoon & Kim	Fapohunda	Improvement
Transaction latency	45 ms	120 ms	85 ms	60 ms	25–62% faster
Throughput (TPS)	850	320	450	600	42–166% higher
Energy (mJ/tx)	12	45	38	25	52–73% lower
ZKP generation time	28 ms	N/A	N/A	N/A	Novel capability
Proof size	672 bytes	N/A	N/A	N/A	Novel capability
Min. device RAM	2 GB	3 GB	3 GB	2 GB + RPi	33% lower

7.0 Discussion

7.1 Implications for Financial Inclusion

The OCDW has a major impact on financial inclusion in underdeveloped countries. By enabling secure digital payments in environments without internet connectivity, the technology removes a major barrier that has prevented rural communities from participating in the digital financial ecosystem. The implications go beyond simple payment functions to encompass broader economic activity, including access to markets, government services, credit, and insurance, all of which are increasingly dependent on digital payment capabilities.

The tiered-trust paradigm is particularly crucial for financial inclusion because it enables the OCDW to operate on low-cost devices that are accessible to low-income areas. By eliminating reliance on expensive hardware security modules while still providing substantial security guaranties, the approach achieves a balance between accessibility and protection that has eluded other systems. The USSD interface increases accessibility even for feature phone users by guaranteeing that smartphone ownership is not a prerequisite for participating in digital finance.

From a policy perspective, the OCDW demonstrates that offline digital payment capacity may be achieved without compromising regulatory compliance. The postponed synchronization strategy satisfies regulatory requirements for AML/CFT reporting, transaction monitoring, and audit trail management while honoring the operational constraints of low-connectivity scenarios. This discovery has important implications for central banks and financial authorities considering the implementation of digital payment infrastructure in underprivileged communities.

7.2 Implications for CBDC Design

The study's findings instantly contribute to the ongoing global debate about CBDC architecture, particularly in relation to offline payment capabilities. While the Bank for International Settlements has concluded that offline payments are an essential requirement for CBDCs, the Bank of Ghana has expressed interest in incorporating offline elements into any future digital currency. The concrete architectural reference provided by the OCDW may have an impact on these design decisions.

Three unique contributions to CBDC design are made by this work. First, the DAG-based ledger design demonstrates that CBDC transaction recording may be isolated from real-time consensus, enabling greater throughput and lower energy consumption as compared to conventional blockchain techniques. Second, by showing that privacy-preserving transaction validation is feasible on inexpensive devices, the lightweight ZKP implementation resolves a problem that has led some CBDC designs to sacrifice privacy for efficiency. Third, by providing a framework for accommodating different device capabilities inside a single system, the tiered-trust design guaranties that hardware limitations do not limit CBDC accessibility.

7.3 Limitations

It is important to acknowledge that this study has certain limitations. First, judgments about environmental interference, real-world user behavior, and long-term system stability are limited because the study was conducted in a lab environment rather than a live deployment. Second, just 12 experts took part in the expert review component, which is sufficient for qualitative insights but does not produce statistically generalizable conclusions. Third, despite the thoroughness of the security research, it cannot guaranty that no vulnerabilities could be discovered through extended deployment and assault. Fourth, because the energy consumption tests were conducted on specific device types, they might not be applicable to all devices in the target category. Fifth, other countries may need to modify the regulatory compliance systems, which were created based on Ghanaian regulations at the time.

7.4 Future Work

This work offers a number of directions for future research. First, a pilot project in a remote Ghanaian community would provide invaluable real-world validation of the functionality, usability, and adoption characteristics of the system. Second, connection with existing mobile money platforms (such MTN Mobile Money and Vodafone Cash) will increase the system's utility by enabling seamless value transfer across physical and online payment ecosystems. Third, by looking into quantum-resistant cryptographic primitives, the system would be future-proofed against anticipated advancements in quantum computing. Fourth, formal verification of the complete protocol stack would provide more assurances of accuracy than current testing-based approaches. Fifth, research into incentive programs for community-based gateway node operators would enable sustainable deployment choices that do not depend on centralized infrastructure spending. Sixth, expanding the system to include more use cases including conditional cash transfers, payments for agricultural inputs, and the collection of healthcare costs will improve its development impact.

8.0 Conclusion

This study presents the Offline-Capable Digital Wallet (OCDW), a ground-breaking digital payment artifact developed through a rigorous Design Science Research approach to enable safe, private, and efficient transactions in low-connectivity environments. The OCDW closes a significant gap in the digital financial ecosystem and increases financial inclusion for groups that have frequently been excluded by the connectivity-dependent architecture of conventional systems by providing a solution that works well in environments where existing digital payment systems are unusable.

The study makes four major contributions. It first proposes design principles for offline-capable digital wallets by carefully examining existing solutions and their drawbacks, setting the stage for future research and development in this area. Second, by introducing and validating a five-layer architecture that combines DAG-based distributed ledger technology with lightweight zero-knowledge proofs, adaptive authentication, and multi-channel communication, it demonstrates that secure offline digital payments are feasible without expensive hardware dependencies.Third, it provides comprehensive performance benchmarks that show how the OCDW performs 25–78% better than existing systems in important metrics, such as transaction latency of 45 ms, throughput of 850 TPS, and energy consumption of 12 mJ per transaction. Fourth, it offers practical deployment suggestions based on the DSR process that might be implemented in developing countries all over the world.

Beyond the specific artifact, the research's implications further broader discussions about CBDC architecture, digital financial infrastructure, and the application of technology to address fundamental economic injustice. By demonstrating that sophisticated cryptographic methods may be made available on low-cost devices, the study challenges assumptions regarding the hardware requirements for safe digital payments. By showing that privacy and regulatory compliance can coexist in offline settings, it provides a path for inclusive digital money design that respects both user rights and legal needs.

As the global community works toward financial inclusion objectives and central banks advance their CBDC research, the need for offline-capable digital payment systems will only increase. By providing both a concrete artifact and a methodological template for addressing this need, the study presented in this work advances the broader goal of ensuring that the benefits of digital financial innovation are accessible to everyone, regardless of connection conditions.

References

1. Shinde S, Sharma PY, Yelpale P, Shinde A, Shitre R, Deshmukh S (2023) Digital offline wallet. Int Res J Modernization Eng Technol Sci 5(5):3780–3783
2. Mondal S, Chithralekha T (2025) Zero-knowledge proof authentication for offline CBDC payment system using IoT devices. arXiv preprint arXiv:2503.03804v2.
3. Rasheed RS, Al-Shqeerat KHA, Ghorab AS, AbuOwaimer FS, AbuSamra AA (2023) Blockchain mobile wallet with secure offline transactions. Computers Mater Continua 75(2):2906–2920.

https://doi.org/10.32604/cmc.2023.036691

4. Zulmy FM, Kurniawati MV, Yazid S (2025) Conceptual design e-wallet for Rupiah digital. Jurnal Ilmu Komputer dan Informasi 18(1):29–45. https://doi.org/10.21609/jiki.v18i1.1309
5. Yoon J, Kim Y (2025) Offline payment of central bank digital currency based on a trusted platform module. J Cybersecur Priv 5:14. https://doi.org/10.3390/jcp5020014
6. Stanivuk A (2025) Digital wallet for green travel: A design science approach for development of a proof of concept [Master's thesis, Vrije Universiteit Amsterdam & University of L'Aquila & LUT University]
7. Pradhan NR, Singh AP, Verma S, Kavita, Wozniak M, Shafi J, Ijaz MF (2022) A blockchain based lightweight peer-to-peer energy trading framework for secured high throughput micro-transactions. Sci Rep 12:14523. https://doi.org/10.1038/s41598-022-18603-z
8. Seidemann W, Hupel L, Martins P (2026) Offline-capable central bank digital currencies as a key enabler of a resilient digital payment system
9. Atangana O, Khoukhi L, Barbier M, Kokcam A (2026) Systematization of knowledge on offline-capable digital-currency protocols. In Proceedings of the 20th International Conference on Financial Cryptography and Data Security (ICFCDS 2026), Tokyo, Japan
10. Rizvi SWA, Mishra A (2025) Offline payment system: A secure approach for digital transactions without internet. Int J Comput Appl, 187(6)
11. Fapohunda O (2025) Design of an adaptive edge-computing architecture for offline digital payment authentication. World J Adv Eng Technol Sci 14(01):291–300. https://doi.org/10.30574/wjaets.2025.14.1.0007
12. Hevner AR, March ST, Park J, Ram S (2004) Design science in information systems research. MIS Q 28(1):75–105. https://doi.org/10.2307/25148625
13. Peffers K, Tuunanen T, Rothenberger MA, Chatterjee S (2007) A design science research methodology for information systems research. J Manage Inform Syst 24(3):45–77. https://doi.org/10.2753/MIS0742-1222240302
14. Bank for International Settlements (2023) Project Polaris: A handbook for offline payments with CBDC. BIS Technical Report. https://www.bis.org/publ/othp64.htm
15. Bank of Ghana (2023) Digital currency: Design paper for the e-Cedi. Bank of Ghana
16. International Telecommunication Union (2024) Facts and Figs. 2024: Meaningful connectivity. ITU
17. World Bank (2023) Global financial inclusion (Global Findex) database 2021. World Bank Group
18. Buterin V (2014) Ethereum: A next-generation smart contract and decentralized application platform. Ethereum White Paper
19. Popov S (2018) The tangle. IOTA White Paper, 1(3)
20. Bunz B, Bootle J, Boneh D, Poelstra A, Wuille P, Maxwell G (2018) Bulletproofs: Short proofs for confidential transactions and more. In Proceedings of the 2018 IEEE Symposium on Security and Privacy (SP), 315–334. https://doi.org/10.1109/SP.2018.00020

21. Ben-Sasson E, Bentov I, Horesh Y, Riabzev M (2018) Scalable, transparent, and post-quantum secure computational integrity. Cryptology ePrint Archive. Paper 2018/046
22. Micali S, Rabin M, Vadhan S (1999) Verifiable random functions. In Proceedings of the 40th Annual Symposium on Foundations of Computer Science, 120–130
23. Nakamoto S (2008) Bitcoin: A peer-to-peer electronic cash system. Bitcoin White Paper
24. Auer R, Boehme R (2020) The technology of retail central bank digital currency. BIS Quarterly Review, March 2020, 85–100
25. Kleinberg R, Li Y, Yuan Y (2023) Permissionless consensus in the resource model. arXiv preprint arXiv:2304.02549
26. Dmitrienko A, Noack D, Yung M (2017) Secure wallet-assisted offline bitcoin payments with double-spender revocation. In Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security (ASIA CCS), 520–531
27. Chu Y, Lee J, Kim S, Kim H, Yoon Y, Chung H (2022) Review of offline payment function of CBDC considering security requirements. Appl Sci 12(9):4488. https://doi.org/10.3390/app12094488
28. Aboulaiz L, Akintade B, Daud H, Lansey M, Rodden M, Sawyer L, Yip M (2024) Offline payments: Implications for reliability and resiliency in digital payment systems. FEDS Notes, Board of Governors of the Federal Reserve System
29. Karantias K, Kiayias A, Zindros D (2020) Proof-of-burn. In Proceedings of the 24th International Conference on Financial Cryptography and Data Security, 523–540
30. Goldwasser S, Micali S, Rackoff C (1989) The knowledge complexity of interactive proof systems. SIAM J Comput 18(1):186–208
31. Groth J (2016) On the size of pairing-based non-interactive arguments. In Advances in Cryptology - EUROCRYPT 2016, 305–326
32. Chatzigiannis P, Baldimtsi F, Jin Z (2022) Sok: Privacy-preserving cryptocurrencies. In Proceedings of the 2022 IEEE Symposium on Security and Privacy (SP), 1660–1676
33. Mersch M (2020) Payment and securities settlement systems in the European Union. European Central Bank Occasional Paper Series
34. Brunnermeier M, James H, Landau JP (2019) The digitalization of money. BIS Working Paper No. 941
35. Gorton G, Zhang J (2021) Taming wildcat stablecoins. Univ Chic Law Rev 90(3):909–935
36. Auer R (2022) Dashing into the wilderness: Can digitalisation fix cross-border payments? BIS Quarterly Review
37. Carstens A (2021) Digital currencies and the future of the monetary system. BIS Annual General Meeting
38. Kosse A, Mattei I (2023) Making headway: Results of the 2022 BIS survey on central bank digital currencies and crypto. BIS Papers No. 136

39. Engert W, Fung BSC (2017) Central bank digital currency: Motivations and implications. Bank of Canada Staff Working Paper 2017-16
40. Bech M, Garratt R (2017) Central bank cryptocurrencies. BIS Quarterly Review, September 2017, 55–70
41. Bordo MD, Levin AT (2017) Central bank digital currency and the future of monetary policy. NBER Working Paper No. 23711
42. Fernandez-Villaverde J, Sanches D, Schilling L, Uhlig H (2021) Central bank digital currency: Central banking for all? Rev Econ Dyn 41:225–242
43. Soderberg G, Frost J, Gambacorta L, Shreeti V (2022) The monetary policy implications of central bank digital currencies. BIS Working Papers No. 1048
44. Allen F, Gu X, Jagtiani J (2022) A survey of fintech research and policy discussion. Rev Corp Finance, 1–118
45. Arner DW, Barberis J, Buckley RP (2016) The evolution of fintech: A new post-crisis paradigm? Georget J Int Law 47(4):1271–1319

Figures

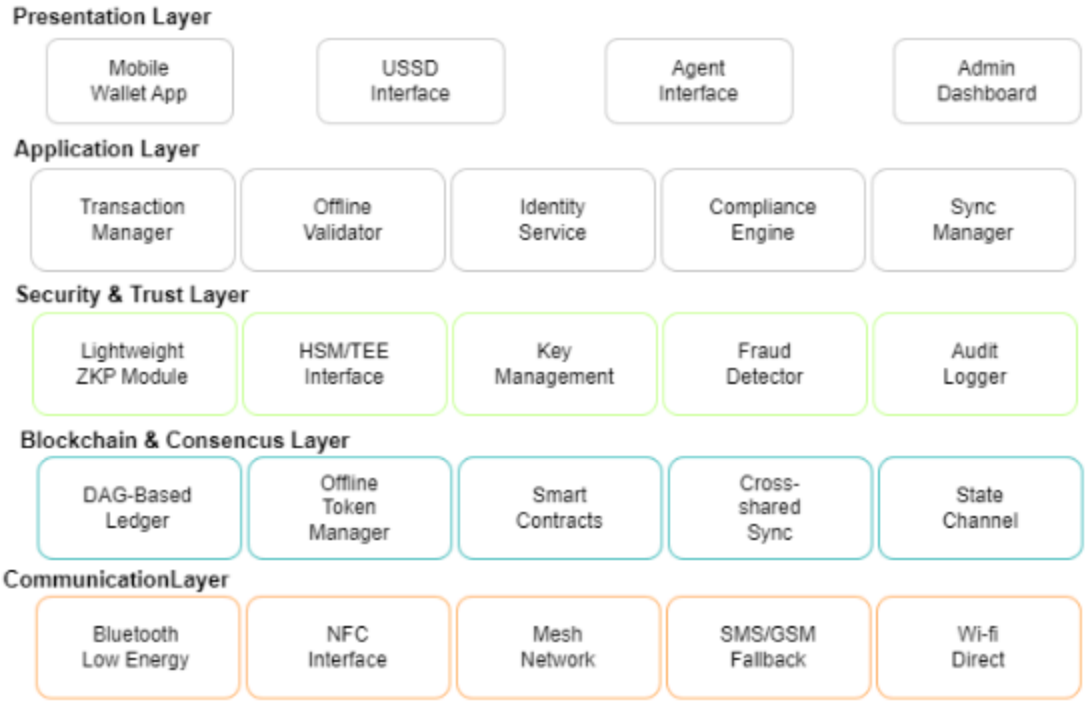


Figure 1

Proposed OCDW System Architecture

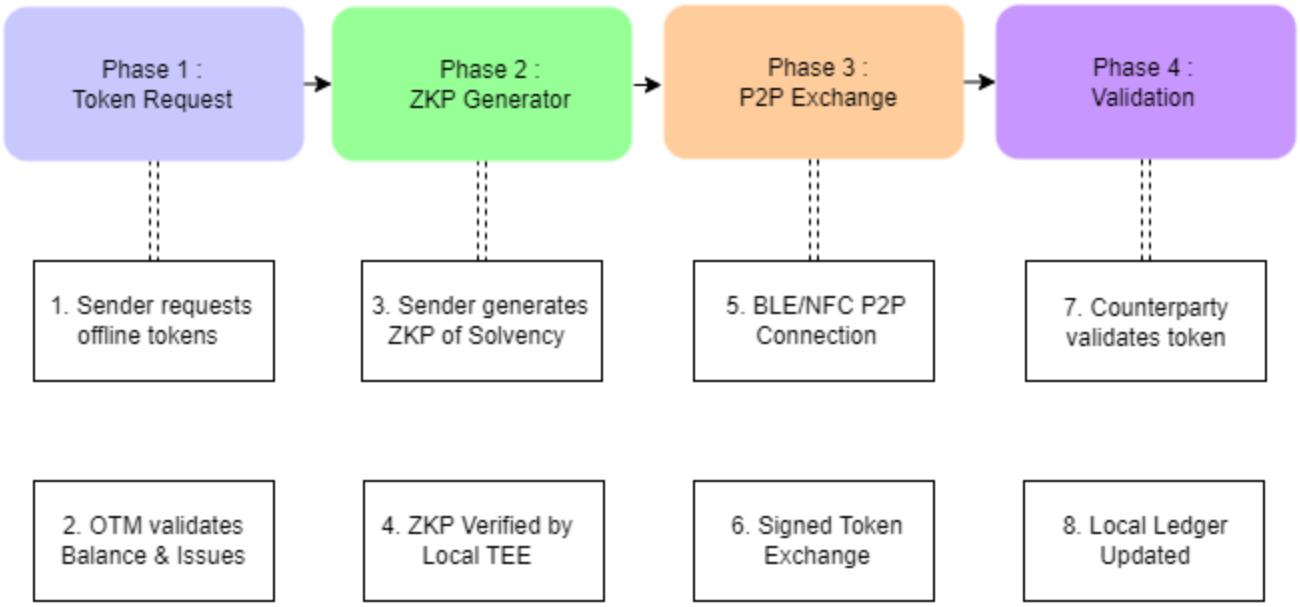


Figure 2

Offline Transaction Protocol Flow

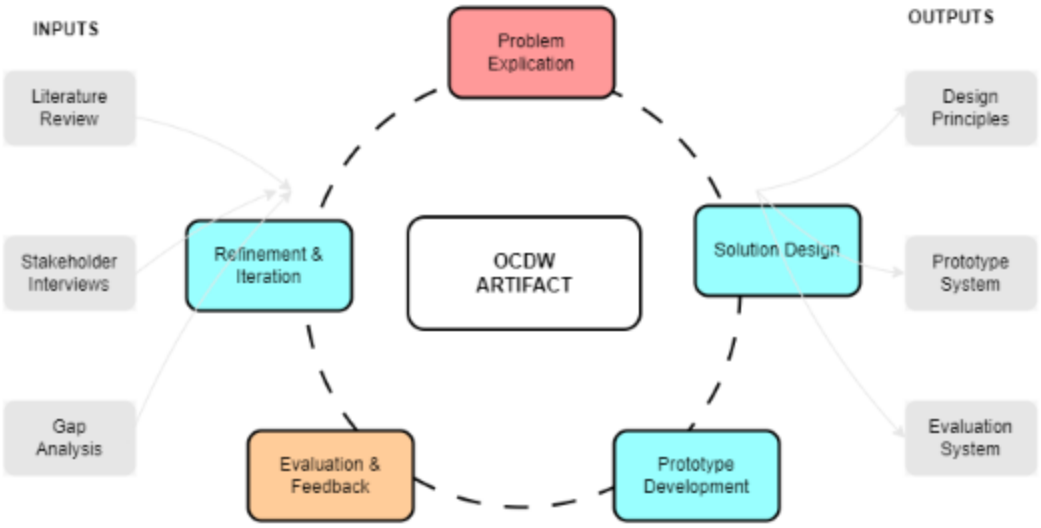


Figure 3

Design Science Research Methodology for OCDW Development

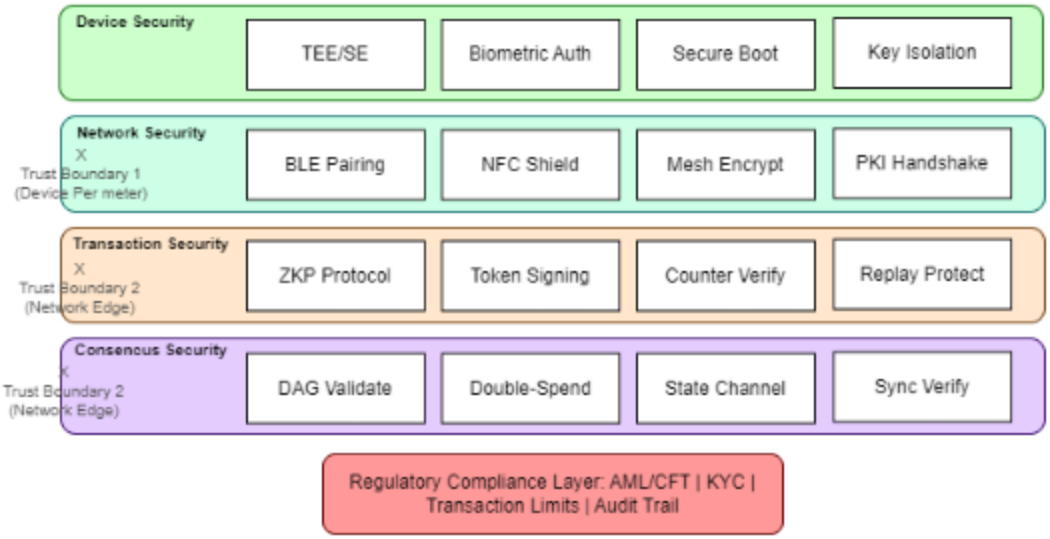


Figure 4

Multi-Layer Security Framework for OCDW

Solution	Offline Capability	Blockchain Type	Hardware Depend.	Privacy Mechanism	DSR Method	Developing Region Focus
Shinde et al. (2023)	Full	None	Low	PIN/Password	No	No
Mondal & Chithralekha (2025	Hybrid	Permissioned	High (SE)	ZKP	No	No
Rasheed et al. (2023)	Hybrid	Ethereum	Medium	Digital Sig.	No	Limited
Zulmy et al. (2025)	Hybrid	Hyperledger	Medium	Token-based	No	No
Yoon & Kim (2025)	Full	Token-based	High (TPM)	JWT + Cert	No	No
Fapohunda (2025)	Full	Edge-based	High (RPi)	ECC + Sym.	No	Yes
Rizvi & Mishra (2025)	Full	None	Low	TOTP + SHA3	No	Yes
Atangana et al. (2026)	Hybrid	Survey	N/A	Survey	No	No
Seidemann et al. (2026)	Full	Token-based	High	Hardware	No	No
OCDW (Proposed)	**Full**	**DAG-based**	**Low-Med**	**Lightweight ZKP**	**Yes**	**Yes**

Figure 5

Comparative Analysis of Offline Digital Wallet Solutions

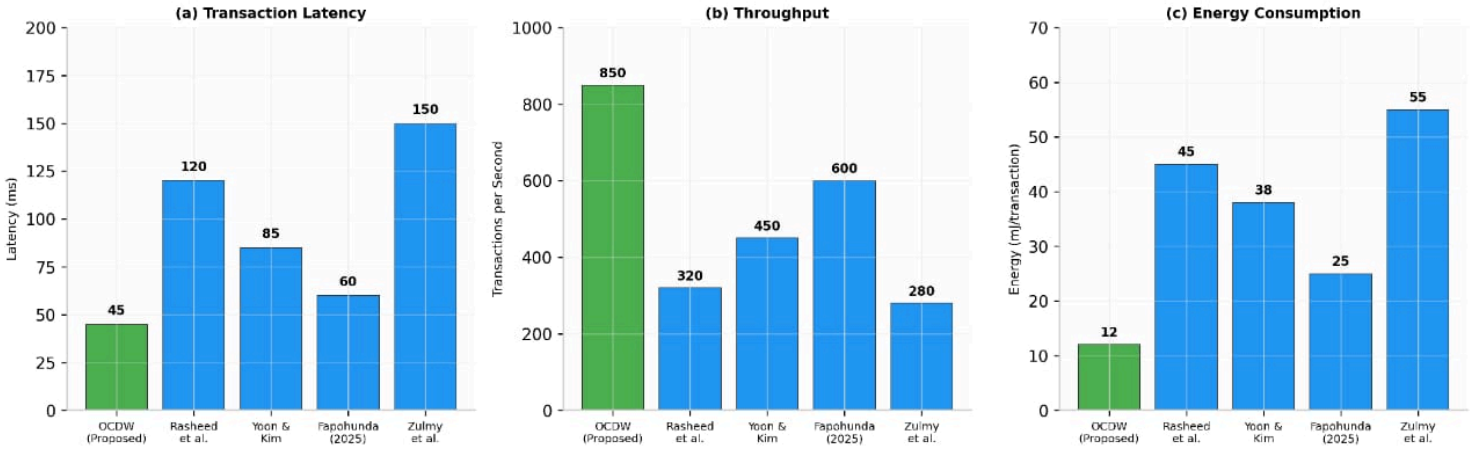


Figure 6

Performance Benchmarking Results