Journal of Trends in Computer Science and Smart Technology (ISSN: 2582-4104)
www.irojournals.com/tcsst/

Review on Blockchain-Based Offline Payment Solutions

Surekha Lanka[1*], Phothiwong Suwannatat[2], Nalinnee Pumhiran[3]

Lecturer, Faculty of Business and Technology, Stamford International University, Bangkok, Thailand.

Email: [1*]Surekha.lanka@Stamford.edu, [2]phothiwong.suwannatat@stamford.edu, [3]nalinnee.pumhiran@stamford.edu

Abstract

Blockchain technology has proven to be a revolutionary base technology for the development of digital payment systems, which include properties like decentralization, transparency, and strong cryptography. However, most existing blockchain-based payment systems require always-connected scenarios, limiting their applicability in environments where no or intermittent internet connectivity is available. Hence, there is increased research in existing studies on blockchain-based offline payment systems, particularly from the viewpoints of financial inclusion and Central Bank Digital Currencies. The objective of this paper is to carry out a detailed review of existing blockchain-based offline payment systems, which includes discussions on design, security, and assumptions. The proposed work will group the prominent existing payment systems along the lines of state channel networks, hardware-based payment systems, and offline token payment systems, which will be analyzed for their pros and cons. In addition, it also raises awareness of prominent security aspects like authentication using cryptography, trusted execution environments, and delayed reconciliation, considering this study to assume certain conditions when examining the offline environment. Finally, based on the major existing work, it will outline important research opportunities in double spending, scalability, privacy, interoperability, and usability. The purpose of this study is, through synthesis, to provide a structured view of the offline blockchain payment platform and help focus R&D efforts on effective, secure, and scalable offline digital payment systems.

Keywords: Blockchain, Offline Payment, Secure Transaction, E-Commerce, Central Bank Digital Currencies, Decentralized Architecture, Digital Wallet, Key Management, Smart Cards.

1. Introduction

Digital payment systems and processes have become an indispensable aspect of the modern finance environment owing to the widespread use of mobile technology, electronic platforms, and the decrease in the use of physical money. However, due to the rapid growth and popularity of cryptocurrencies and blockchain-based digital payment systems, it has been observed that this technology has the ability to ensure significant resistance to centralization and can facilitate peer-to-peer payments across geographical locations. Despite the benefits and advantages arising from the use of blockchain digital payments, the fact remains that most blockchain digital payment systems currently require and support an online connection. Such dependence on an online connection can be considered an enormous drawback for blockchain

* **Corresponding Author**

DOI: https://doi.org/10.36548/jtcsst.2025.4.008
Received: 10.11.2025, received in revised form: 08.12.2025, accepted: 22.12.2025, published: 02.01.2026

digital payment systems since this technology will not work in the absence of an internet connection. This aspect makes a significant negative distinction between money and blockchain digital money.

This has made offline payment services a major area of research interest, especially given the increasing interest of the global community in Central Bank Digital Currencies (CBDCs). Indeed, for a CBDC to be a proper digital alternative to money, it to provide safe and efficient offline payment services. In this regard, the choice of blockchain technology appears more favorable compared to other systems of offline digital money because of the availability such as features of integrity-proof record management, deferred verification, and adherence to a set of rules upon reconnection after offline status. The question of implementing offline payment services, therefore, poses many complex problems for systems based on the blockchain technology. Without the need for a common shared ledger in real time, double-spending must be avoided, a transaction must be authenticated, and this must be consistent with the underlying blockchain after connectivity is restored. Among these, a variety of blockchain-based offline payment schemes have been proposed, relying on different paradigms, such as trusted hardware and secure elements, smart cards, off-chain payment channels, delay-tolerant networking, and even hybrid architectures that combine local transaction execution with eventual on-chain settlement. While each of these approaches offers unique benefits, they also imply fundamental trade-offs in terms of the trust model, system complexity, scalability, and deployment feasibility. Consequently, no single solution has seen general adoption, leaving the design space fragmented.

This article presents a detailed review of blockchain-based offline payment solutions by systematically examining their underlying architectures, security mechanisms, and operational assumptions. Unlike prior studies that primarily focus on isolated system designs or specific use cases, this review addresses key research gaps by (i) providing a unified classification of offline payment approaches across different trust and deployment models, (ii) explicitly analyzing the often-implicit operational assumptions such as bounded offline duration, device trustworthiness, and economic risk tolerance that underpin system security, and (iii) identifying limitations in existing solutions regarding scalability, reconciliation, and real-world usability. By synthesizing current research and highlighting open challenges, this review aims to support researchers, practitioners, and policymakers in advancing practical, resilient, and inclusive offline blockchain payment systems.

2. Literature Review

Research on blockchain-based offline payment systems has intensified due to the growing limitations of always-online digital payments. One of the notable initiatives is the Pure Wallet (PW) architecture [1] which proposes an offline transaction model that stores transactions temporarily on user devices and synchronizes with the blockchain ledger when connectivity is restored. This model demonstrates technical feasibility while raising concerns regarding secure local storage and the prevention of double spending during offline periods.

The relevance of offline payment capabilities is especially pronounced with the emergence of central bank digital currencies (CBDCs). [2] analyzes offline CBDC payments, identifying essential security requirements such as transaction integrity, user authentication, and fraud resistance. They indicate that while offline payments enhance usability, they depend on trusted components that can undermine the decentralized attributes of blockchain systems. Furthermore, [3] advocates for a smart card-based approach to offline CBDC transactions,

embedding secure elements in cards to enforce spending limits and prevent unauthorized fund reuse. Although this design offers robust security, it introduces dependency on specialized hardware and centralized issuance, limiting system flexibility.

[4] provides architectural guidance for blockchain payment systems by identifying common patterns used in blockchain-based payment applications, which include off-chain processing and trust boundary separation. Although their study does not focus exclusively on offline payments, it lays a foundational framework for designing systems capable of managing temporary disconnection while ensuring alignment with the blockchain ledger.

Another significant research avenue pertains to off-chain mechanisms and payment channels. [5] reviews blockchain-based payment channel networks that can diminish latency and transaction costs. Although these channels are primarily designed for online use, their principles influence offline payment solutions. [6] proposes a delay-tolerant payment method based on Ethereum, illustrating that transactions can proceed with limited connectivity, deferring validation until network access is available. Nonetheless, they acknowledge challenges, including settlement delays and security risks during offline operations.

Security challenges within offline payment environments extend to the realm of payment terminals and user devices. [7] examines system-wide security protocols for offline payment terminals, advocating for an integrated security design that encompasses hardware, software, and communication layers to mitigate threats such as replay attacks and device cloning. This perspective addresses the necessity for offline blockchain payments to address not only cryptographic protocol vulnerabilities but also deployment risks.

Recent advancements seek to enhance the usability of offline digital payments. [8] introduces ElasticPay, a peer-to-peer offline payment system that allows instant transactions without ongoing connectivity. This system emphasizes speed and flexibility suitable for real-world consumer applications, although the long-term coherence with distributed ledgers remains unresolved. [9] discusses the potential of blockchain in facilitating CBDCs, highlighting offline payment capability as vital for public acceptance, especially in network outages or remote locales.

[10] discusses a consortium blockchain-based digital currency aimed at cross-border payments, concentrating on auditability and interoperability. Their proposed architecture sheds light on how controlled, permissioned contexts could enhance offline or semi-offline payment systems. Collectively, these studies reveal that varied approaches to offline payments exist, yet none completely reconciles the trade-offs among security, decentralization, usability, and scalability, leaving considerable room for further research into resilient offline payment mechanisms within blockchain frameworks.

Recent advancements in blockchain-based security frameworks demonstrate their growing significance across image authentication, offline payments, mobile commerce, healthcare data management, and IoT marketplaces. The BlockImage framework introduces a secure and intelligent approach for image authentication and provenance by integrating artificial intelligence with blockchain technology, ensuring tamper resistance, traceability, and trust in digital image ownership and verification processes, which is particularly relevant for combating image forgery and misinformation [16]. In parallel, blockchain-based offline payment protocols have gained attention for addressing reliability and security challenges in disconnected environments, where cryptographic guarantees, double-spending prevention, and flexible transaction validation mechanisms enable secure financial operations without

continuous network connectivity [17]. These developments align closely with security-driven evaluations of Central Bank Digital Currency (CBDC) offline payment functionalities, which emphasize confidentiality, integrity, availability, and resilience against fraud while maintaining usability and regulatory compliance [18]. Beyond financial systems, blockchain adoption in mobile payments has been systematically reviewed, highlighting its role in enhancing transaction transparency, decentralization, identity protection, and fraud mitigation in mobile commerce ecosystems, thereby strengthening user trust and system robustness [19]. Furthermore, blockchain-enabled open-source tools for managing electronic health records (EHRs) provide secure data sharing, fine-grained access control, interoperability, and auditability in hospital environments, addressing persistent challenges related to privacy, data integrity, and regulatory compliance in healthcare systems [20]. Collectively, these studies illustrate the versatility of blockchain technology as a foundational layer for secure digital services, demonstrating its effectiveness in ensuring trust, privacy, and resilience across diverse application domains including multimedia authentication, financial transactions, healthcare information systems, and IoT-driven marketplaces.

3. Architecture of Blockchain-Based Offline Payment System

The design for such an offline payment system utilizing blockchain technology helps ensure financial transactions securely when there is less or no connectivity to the internet, without compromising on elements such as trust, transparency, and integrity of the blockchain concept. The design applies cryptocurrency techniques, processing, and the concept of deferred validation for synchronizing transactions on the blockchain.

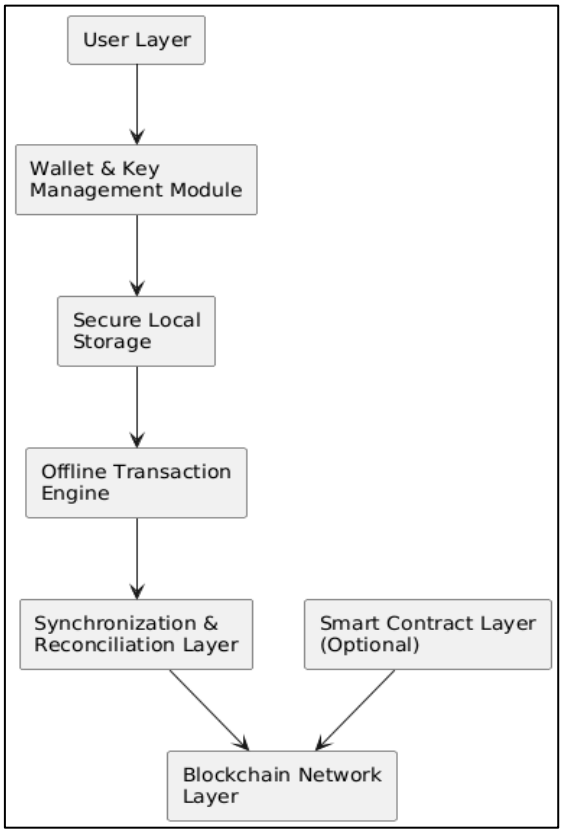

Figure 1. Architecture of a Blockchain-Based Offline Payment

The user layer interacts with devices such as mobile phones, smart cards, or point-of-sale machines with a light wallet running blockchain technology. This layer enables users to conduct offline peer-to-peer payments through digital signatures of the transaction for authentication, as well as secure handling of private keys by hardware components. This wallet and key management layer is responsible for managing the generation of cryptographic credentials. This makes it easy to digitally sign and secure the transaction using techniques such as one-time keys and multi-signature systems. At the level of processing the transaction offline, transaction processing occurs without necessarily using blockchain technology at that moment, and necessary transaction details are stored. There is a reduced risk of double spending due to pre-funded wallets and/or vouchers.

A secure local storage mechanism is also implemented, which retains all offline transactions securely until connectivity is established, using encryption and tamper-resistant storage for secure processing and employing checks for any malicious manipulation during the process. When connectivity is restored, the synchronization and reconciliation mechanism is used for submitting offline transactions to the blockchain for validation and processing, handling double spending issues and wallet balance adjustments based on validation. The blockchain-network mechanism is also implemented for validation, consensus, and updating the ledger for trusted interactions among users during synchronization for offline transactions. An optional smart contract layer could be included to facilitate automated payment policies, spending limits, and transaction terms. Thus, an optional smart contract layer could be included to improve payment transparency and fairness. Overall, this architecture combines the best practices of decentralized blockchain technology with offline features to deliver reliable payment solutions that would be difficult to attain when an internet connection is a requirement.

This is because the longer the time that an individual is offline, the higher the risk of attacks such as key compromise, illicit balance adjustment, and replay attacks. There is also a threat to the offline transaction processing layer because the transaction data parameters such as limits and state are not immediately able to be validated by the global ledger. This poses a greater risk of state inconsistencies and double spending. Another layer that is threatened is the secure storage layer because it is vulnerable to attacks such as data tampering, rollback attacks, and storage exhaustion attacks as a result of the accumulation of transaction data that is stored offline.

4. Existing Approaches to Blockchain-Based Offline Payments

The offline payment systems based on blockchain technology can be classified into two categories, which have varying levels of architecture and security. The systems make extensive use of advanced cryptographic techniques and existing contracts on the main blockchain to allow for the execution of offline payments.

4.1 State Channels (eg. Lightning Network)

State channels enable two or more participants to carry out several transactions off the blockchain once the participants lock their funds in a smart contract on the blockchain. Implementations like the Lightning Network and Raiden Network include cryptographically signed modifications exchanged among members, which allows for payments without much lag or fees [14]. Although the initial implementation for state channels was intended for use

online, they can be adapted for offline processing, considering the communication mechanism via members (e.g., Bluetooth and/or NFC) [6].

Table 1. Strengths and Limitations of State Channels

Strengths	Limitations
Transactions are nearly instantaneous and incur no per-transaction fee, dramatically increasing throughput.	Funds must be locked onto the main chain, reducing capital efficiency.
Security is guaranteed by the main chain's smart contract and cryptographic signatures.	For true security, an online "watchtower" must monitor the chain for fraud attempts if a party goes offline, adding a layer of complexity.
Only the opening and closing transactions are broadcast publicly; all intermediate transactions are private.	Channels must be opened, funded, and maintained (which may require fees), making spontaneous or one-off payments difficult.
Does not rely on a single central entity for transaction validation.	For payments between parties who don't have a direct channel, a complex network of channels must route the transaction.

Strengths and weaknesses of state channel-based solutions are summarized above Table 1. One of the major advantages is that the solution offers excellent security because although there may be fraud, it is all sorted out using on-chain dispute resolution once the channel is restored. One of the drawbacks of the solution is that, because lockups are on-chain, there is less liquidity, and using watchtowers increases the complexity of the solution when parties are offline for a longer period of time.

4.2 Trusted Execution Environments (TEEs) and Secure Elements (SEs)

The schemes based on trustworthy hardware use tamper-resistant parts (either smart card or secure element, or Trusted Execution Environment/TEEE), which are trustworthy with regard to their execution in enforcing co-locally the spending conditions. The private information and the offline balances are maintained in the trustworthy hardware, and authorization of transactions happens via cryptographically protected device-to-device communication [7]. These schemes receive special attention, especially within the scope of offline CBDCs, to provide properties typical of physical money using smart card or secure wallet technology [2], [11].

Table 2. Strengths and Limitations of Trusted Execution Environments and Secure Elements

Strengths	Limitations
The secure hardware makes it extremely difficult to access the private key or forge the transaction log, solving the central offline security problem.	Security relies heavily on the integrity of the chip/hardware manufacturer (hardware root of trust), introducing a form of centralized trust.
The transaction can be considered final at the moment of the secure exchange, similar to cash.	Requires specialized, certified hardware, increasing the cost and complexity of deployment compared to purely software-based solutions.

Provides robust security even in environments with zero connectivity.	TEEs, while secure, have been subject to complex side-channel attacks (e.g., Spectre, Meltdown) that could potentially leak sensitive information.

As seen in Table 2, side-channel attacks utilize the leakage of sensitive information through incomplete channels, including timing variations and power consumption, to reveal private information about secure hardware. There have been prominent attacks, including the Spectre and Meltdown attacks, which showed that even Trusted Execution Environments and Secure Processors are vulnerable to the leakage of cryptographic keys without attacking the cryptographic security. Vulnerabilities in offline payment systems mean an attacker can manipulate private keys, account balances, or even the records of transactions within an unattended or hostile environment.

4.3 Intermediary-Based/Token Solutions (Hybrid)

By using intermediary-based solutions, there is the concept of a trusted or semi-trusted party named the Offline Token Manager (OTM) who is responsible for the issuance of offline tokens. Users will receive a fee for exchanging their online currency into cryptographically signed offline tokens. These tokens can be transferred in a peer-to-peer fashion when the system is offline. They will be redeemed as soon as the system is online again [8], [10]. This type of solution is almost the same as a digital cash system.

Table 3. Strengths and Limitations of Offline Token Manager Systems

Strengths	Limitations
The user experience is straightforward, mimicking the use of cash or a prepaid card.	The OTM (or a central issuer) is a highly trusted entity responsible for not double-issuing OTs and honouring redemptions.
Modern approaches allow the tokens to be securely split or redeemed for change during offline transactions.	If the OTM is compromised or malicious, the entire pool of offline funds is at risk.
Can be implemented over various P2P communication channels (Bluetooth, QR).	If not designed carefully, these systems are susceptible to the generation of fake offline tokens by malicious users.

From Table 3, it can be concluded that OTM-based systems, which offer a similar experience to that of cash, infer a loss of decentralization due to a trust factor on the token issuer. Hence, it can be concluded that the entire security of this system depends on the integrity, availability, and non-compromise of the OTM. Such a system would be best suited for a permissioned environment, like CBDC [9,10].

Table 4. Existing Approaches to Blockchain-Based Offline Payments: A summary

Feature	State Channels	TEE/SE Solutions	OTM Solutions
Decentralization	High	Medium	Lowest
Security Mechanism	Cryptographic state updates & Watchtowers	Hardware isolation & Secure Storage	Centralized Token Management & Signature Check

Double-Spend Risk	Prevented by on-chain fraud proofs	Prevented by hardware tamper-resistance	Prevented by OTM-issued unique tokens/revocation lists
Resilience/Finality	High, but requires eventual on-chain settlement	Highest, immediate offline finality	High, but redemption requires OTM's service

Table 4 shows the three broad categories of the blockchain offline payment system. State channel solutions have the highest level of decentralization, but their finality on the blockchain and continuous observation depend on other factors. The offline finality is strongest for the TEE/SE solutions, but the mechanism is based on hardware trust assumptions. The operational simplicity causes centralization of control and the problem of systemic risk for the other two schemes.

5. Security Mechanisms and Operational Assumptions in Blockchain-Based Offline Payment Systems

There is a combination of common security mechanisms and assumptions in the existing literature, that formulates the security model of the blockchain system's offline payment process. The offline aspect of the payments depends mainly on the application of digital signatures and cryptographic authentication for authenticity and non-repudiation of transactions. For the receiver to confirm the authenticity of the sender without accessing the internet, the offline transaction has to be signed via the private keys held either in the wallets or the secure devices [1], [6]. The concept of the transaction counter and the application of hash chaining help to maintain the integrity of the transactions during the offline process [8].

Among the foremost security primitives existing for the aforementioned offline transaction systems and other similar systems being proposed today is the use of trusted hardware ranging from smart cards to secure elements, and more recently, trusted execution environments. Smart-card based CBDC systems, as an example, rely on the presumption that the hardware setup and key storage provide sufficient tamper resistance to ensure that the offline balances cannot be copied or forged. Similarly, TEE-based systems, for example, the asynchronous payment systems, presume that enclave execution takes place properly and is not compromised.

In most offline payment systems, the goal is to provide the same levels of privacy as physical money while still providing accountability. Using pseudonyms, un-linkable transfer tokens, and limited disclosure credentials have been proposed as methods that would allow privacy to still exist in offline systems [2], [9]. However, most of them assume that anonymity requires certain conditions—namely that the anonymity is guaranteed post-transaction auditability upon the request of regulatory and legal parties when the synchronizations are done.

5.1 Operational Assumptions

Across the literature, several operational assumptions underpin the feasibility of offline blockchain payments, as shown in the table below.

Table 5. Operational Assumptions

References	Operational Assumption	Description
[1], [6]	Bounded Offline Duration	Users are assumed to reconnect to the network periodically, allowing offline transactions to be reconciled, validated, and fraud to be detected.
[2], [9]	Economic Risk Tolerance	The system tolerates limited financial losses from potential double spending, which is considered acceptable for low-value or retail transactions.
[3], [7]	Device Trustworthiness	Wallets, payment terminals, and smart cards are assumed to be secure, non-malicious, and resistant to physical or logical tampering.
[2], [9]	Policy and Governance Support	Offline payment systems, particularly for CBDCs, assume oversight by central banks, including rule enforcement, transaction monitoring, and revocation authority.
[4], [8]	User Compliance	Users are expected to follow system rules, such as respecting transaction limits and performing timely synchronization after offline use.

5.2 Implications of Assumption Violations

The security of offline blockchain payment systems is heavily reliant on operational assumptions that, if violated, can lead to significant vulnerabilities. Key issues include the potential for double spending if the bounded offline duration assumption fails, as attackers could exploit this lapse before reconciliation [2]. If device integrity is compromised due to malware or tampering, locally enforced limits become ineffective. Additionally, exceeding the anticipated economic risk can cause systemic losses and damage public trust, particularly in CBDC implementations [3]. Moreover, insufficient user compliance, such as synchronization delays or deviations from protocols, can result in inconsistent ledger states and unresolved disputes. These factors underscore the necessity for offline payment systems to be designed in such a way that they can gracefully handle assumption violations, incorporating mechanisms for recovery, revocation, and accountability.

6. Open Research Challenges

A contribution of offline blockchain payment solutions is to enable the exchange of value even if the system is not connected to the blockchain. While the literature at present indicates that this is possible, the problem of successfully implementing the solution is still pending. From the literature regarding offline wallets, CBDC, payment channels, and delay-tolerant networks, it is clear that certain open problems lie in this area and need to be solved.

The key challenge posed by double-spending prevention has been, and still is, the most basic challenge associated with offline blockchain payments. The verification of transactions has always been dependent on global consensus within a real-time setting. Therefore, offline transactions have continued to affect such verification processes. The methods discussed that apply based on secure hardware wallets, counters, or time-limited spending tokens address this challenge but cannot fully eradicate it [1], [2]. Some of these offline payment systems rely on

trusted execution environments, smart cards, and secure elements for spending conditions [3], [11]. However, this has continued to exert high levels of trust on the parties offering these products [7].

After restoring connectivity, the challenge of settling offline transactions relative to the blockchain is encountered. Maintaining consistency and resolving contention and refused transactions have been some of the issues that have remained at hand. Bounded offline times and probabilistic acceptance are the strategies that most state-of-the-art techniques leverage. Scaling down to millions of users and devices is required by most offline payment systems, along with low storage, computation, and energy requirements. Furthermore, storing transaction data, proof of cryptographic validity, and spending certificates locally is not practicable.

Solutions on the second layer, such as payment channels and off-chain networks, improve scalability but typically require intermittent or asynchronous access to the blockchain, not fully offline operation in general scenarios [13], [14]. Integration between offline payments and L2 scalability technologies raises several new challenges for ensuring liquidity, channel security, and guarantees for delayed settlement. Limits on transactions, spending, or validity periods are most commonly applied in proposals for offline payments, focusing on optimal values for fraud control versus usability within the context of disparate economic environments, such as cross-border transactions, and are recognized as an open problem [10].

Offline payment transactions are more involved regarding the trade-off between privacy and regulatory control. Though privacy is expected in cash-like payments, the government wants auditability and traceability in certain cases [2]. The existing system fails to maintain compliance with the above conditions without making the system dependent on being online and/or making the system central and traceable. In addition to the security aspect, the offline payment system needs to be friendly and functional in the presence of intermittent power, unreliable hardware, and user errors [4], [8].

7. Conclusion

Offline payment systems based on blockchain are essential for the increased usage of digital money in disconnected settings. This review highlights the importance of the architecture, security, and functionality of current offline payment systems, as the compromise between offline usage and the security of the blockchain is a key focus of ongoing research. There are multiple ways to achieve offline payment systems, such as the use of state channels and smart cards. However, the current solutions require a limited period of being offline while relying on trusted third parties, thus contradicting the goal of increased digital money usage. The key challenges include protection against double-spending, safe reconciliation, privacy maintenance, and the existing infrastructure of payment systems.

References

[1] Igboanusi, Ikechi Saviour, Kevin Putra Dirgantoro, Jae-Min Lee, and Dong-Seong Kim. "Blockchain Side Implementation of Pure Wallet (PW): An Offline Transaction Architecture." ICT Express 7, no. 3 (2021): 327-334.

[2] Chu, Yeonouk, Jaeho Lee, Sungjoong Kim, Hyunjoong Kim, Yongtae Yoon, and Hyeyoung Chung. "Review of Offline Payment Function of CBDC Considering Security Requirements." Applied sciences 12, no. 9 (2022): 4488.

[3] Doğan, Ali, Mustafa Takaoğlu, and Taner Dursunand Ercan Ölçer. "Smart Card Based Offline Payment System for Central Bank Digital Currencies." Edited by Sergey Y. Yurish (2022): 114.

[4] Lu, Qinghua, Xiwei Xu, HMN Dilum Bandara, Shiping Chen, and Liming Zhu. "Patterns for Blockchain-Based Payment Applications." In Proceedings of the 26th European Conference on Pattern Languages of Programs, 2021, 1-17.

[5] Papadis, Nikolaos, and Leandros Tassiulas. "Blockchain-Based Payment Channel Networks: Challenges and Recent Advances." IEEE Access 8 (2020): 227596-227609.

[6] Hu, Yining, Ahsan Manzoor, Parinya Ekparinya, Madhusanka Liyanage, Kanchana Thilakarathna, Guillaume Jourjon, and Aruna Seneviratne. "A Delay-Tolerant Payment Scheme Based on the Ethereum Blockchain." Ieee Access 7 (2019): 33159-33172.

[7] Ivanov, Nikolay, and Qiben Yan. "System-Wide Security for Offline Payment Terminals." In International Conference on Security and Privacy in Communication Systems, Cham: Springer International Publishing, 2021, 99-119.

[8] Reddy, Annapureddy Venkata Sai Kumar, and Gourinath Banda. "ElasticPay: Instant Peer-to-Peer Offline Extended Digital Payment System." Sensors (Basel, Switzerland) 24, no. 24 (2024): 8034.

[9] Zhang, Tao, and Zhigang Huang. "Blockchain and Central Bank Digital Currency." Ict Express 8, no. 2 (2022): 264-270.

[10] Islam, Md Mainul, Md Kamrul Islam, Md Shahjalal, Mostafa Zaman Chowdhury, and Yeong Min Jang. "A Low-Cost Cross-Border Payment System Based on Auditable Cryptocurrency with Consortium Blockchain: Joint Digital Currency." IEEE Transactions on Services Computing 16, no. 3 (2022): 1616-1629.

[11] Lind, Joshua, Oded Naor, Ittay Eyal, Florian Kelbert, Emin Gün Sirer, and Peter Pietzuch. "Teechain: A Secure Payment Network with Asynchronous Blockchain Access." In Proceedings of the 27th ACM Symposium on Operating Systems Principles, 2019, 63-79.

[12] Saputhanthri, Amila, Chamitha De Alwis, and Madhusanka Liyanage. "Survey on Blockchain-Based IoT Payment and Marketplaces." IEEE Access 10 (2022): 103411-103437.

[13] Zhang, Yuhui, Dejun Yang, and Guoliang Xue. "Cheapay: An Optimal Algorithm for Fee Minimization in Blockchain-Based Payment Channel Networks." In ICC 2019-2019 ieee international conference on communications (icc), IEEE, 2019, 1-6.

[14] Gangwal, Ankit, Haripriya Ravali Gangavalli, and Apoorva Thirupathi. "A Survey of Layer-Two Blockchain Protocols." Journal of Network and Computer Applications 209 (2023): 103539.

[15] . R., Sathyabama A, and Jeevaa Katiravan. "BlockImage: A Secure Framework for Image Authentication and Provenance Using AI and Blockchain." Journal of Innovative Image Processing 7, no. 1 (2025): 28-49

[16] Jie, Wanqing, Wangjie Qiu, Arthur Sandor Voundi Koe, Jianhong Li, Yin Wang, Yaqi Wu, Jin Li, and Zhiming Zheng. "A Secure and Flexible Blockchain-Based Offline Payment Protocol." IEEE Transactions on Computers 73, no. 2 (2023): 408-421.

[17] Chu, Yeonouk, Jaeho Lee, Sungjoong Kim, Hyunjoong Kim, Yongtae Yoon, and Hyeyoung Chung. "Review of Offline Payment Function of CBDC Considering Security Requirements." Applied sciences 12, no. 9 (2022): 4488.

[18] Rattanawiboonsom, Vichayanan, and Nohman Khan. "Blockchain Technology in Mobile Payments: A Systematic Review of Security Enhancements in Mobile Commerce." International Journal of Interactive Mobile Technologies 18, no. 21 (2024).

[19] . Shaik, Zahid Hussain, and Kelapati poonia. "A Comprehensive Review of Blockchain-Enabled Open-Source Tools for Managing Electronic Health Records (EHR) in Hospitals." Journal of Trends in Computer Science and Smart Technology 7, no. 3 (2025): 498-516.

[20] Saputhanthri, Amila, Chamitha De Alwis, and Madhusanka Liyanage. "Survey on Blockchain-Based IoT Payment and Marketplaces." IEEE Access 10 (2022): 103411-103437.