Deep Science Publishing
https://doi.org/10.70593/978-81-989050-1-7_3

DeepScience
Open Access Books

Chapter 3: Architectural innovations in instant settlement networks and secure payment gateways

3.1. Introduction

The increasing use of digital technologies for settlements calls for review of the available implementations for usability and security to develop a framework for these applications that, when followed, generates gateways apt for secure operations. The intervention of trusted third parties and the currently prevalent insecure methodologies for instant settlements are sources of annoyances and of an open window for attackers, resulting in system or user vulnerabilities. The purpose of this chapter is double: first, it aims at reviewing implementations of recently proposed schemes for use by gateways apt for secure payments; second, it proposes a set of security rules for designing, developing and maintaining such gateways, based on previously identified vulnerabilities .

The proposal of architectures for secure payment gateways constitutes the first step for developing methods and protocols for secure payments. Deciding on the bases used for their operation and the building-blocks, like for example the one-to-many operations or the to-amount operations, help in clarifying the system operation rules, especially the entity or entities from which the money has to be debited or credited. These architectures must also define the formal structure of their APIs, so that any system constituent entity can freely develop the system modules, based on the available APIs. In addition to this initial step, the proposal of necessary attributes for establishing, maintaining and securing the inter-relations among those entities and their owners, is also essential for ensuring the secure system operation. Analyzing these cross-entity attributes allows to prove protocol security. Finally, it must also be defined who guarantees that all those attributes and cross-entity relations are correctly set and secured, at system initiation and during its operation, so that the transactions granted by the gateways are indeed valid (Carstens & Nilekani, 2024; Malempati, 2024; Mwale & Phiri, 2024).

Central banks are not often considered in this light. While autonomous central banking may be desirable, the present tendency to rely upon automatic balancing devices, by

which money in the form of bonds is pulled into general use when prices are falling and is pushed into long-term investments when expenses are excessive, may help to avoid too wide fluctuations in the level of economic activity but does little to save society from the costly disruptions that are inevitably connected with the small numbers involved in suffering the immediate consequences of abrupt changes in the movement of prices, or with the misallocation of resources that results in the conflict referrals into public hands of insolvencies and the resource misallocation that creates doomsday scenarios. If too much information establishes a need to recapture, what creates excess or disperse application are credit policies adopted too early or too late (Bojjagani et al., 2023; Hefny et al., 2023).

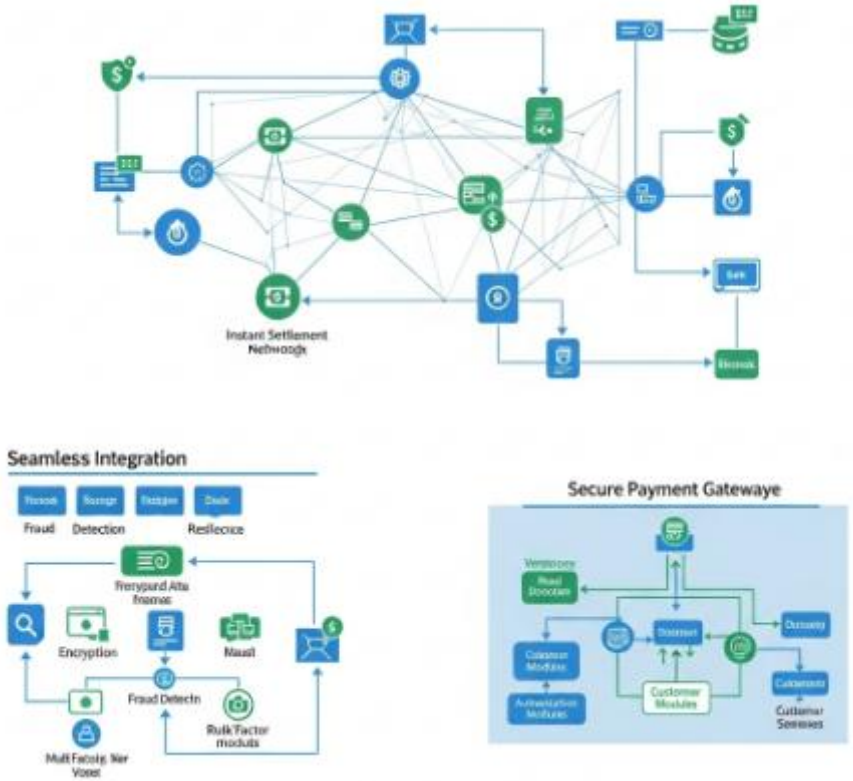

Fig 3.1: Architectural Innovations in Instant Settlement Networks

3.1.1. Background and significance

The central economic problem facing modern societies is how to allocate scarce resources to satisfy unlimited wants. This can only be solved by employing a reliable system that permits free individuals to communicate preferences through market prices and to give each agent incentives to produce according to these expressed desires.

Market prices must, therefore, contain information. Economic theory identifies the likely source of errors in the allocation of resources in a free enterprise economy that are likely to result in erroneous cost estimates of production - altered market prices, which occur when demand increases sharply relative to supply and create temporary shortages of goods. Until relatively recently, however, economists have ignored the precautionary motive behind demand and have assumed that demand is exclusively determined by the need for the goods themselves. When supply is temporarily allowed to remain less than demand, then relatively few producers are priced out of the market and their loss is felt as a tragic disaster. However, beyond the immediate loss, the diversion of resources to less productive uses results in a net loss to the entire economy, and this would need to be recouped, before the process begins again.

3.2. Background of Payment Systems

Banks and regulated payment services providers maintain payment systems that have settled different types of payment contracts in a number of currencies. A conventional bank is a legal entity, chartered by a regulatory agency to receive deposits and make loans under a legal framework including capital requirements. Non-bank payment services providers can offer payment services in specialized markets, but they are usually regulated according to the type of services they offer and as against regulated banks. Such regulation may take the form of requiring the non-bank payment service provider to hold funds deposited by clients in escrow accounts with banks while the non-bank facilitator offers payment services to customers, or by requiring the non-bank payment service provider to keep certain amounts in reserve, and restricting its use of such amounts. Such regulation aims to reduce fraud, the risk of loss to the consumer, and to promote financial stability.

Payment systems date back to the very origins of civilization. In contrast to the simple exchange of goods and services, which is usually called barter, urban civilization required a more sophisticated means of exchange. Dollars, yen, and euro notes circulate from hand to hand, but their value arises from both the labor costs involved in their manufacture and the ultimate guarantees of the issuing government to redeem their value from the public. Banks can issue notes, but they are eclipsed by central banks who acquire leading currencies within national borders bearing the sovereign guarantee. They are able to draw demand for such notes and deposits trusting in the long term ability of their government to redeem the value of their currency in terms of lasting universal assets: commodities whose scarcity restricts their availability, and time, whose short term availability will be depleted in exchange for everlasting rewards. The real world payment gateways connecting depositors with fund recipients at call are micro services

visiting on demand in the real world for a fee, while gate services connect depositors with fund recipients in the virtual world via the Internet.

3.2.1. Research design

In Section 3.2.1, the present study utilizes a qualitative research methodology. The sample of this qualitative study consists of 24 highly experienced individuals selected based on their unique expertise and wide-ranging experiences with payment systems and networks. Interview participants were chosen based on their years of service, grade level, trove of specialized expertise, and their depth of institutional and cultural experiences in governmental, industry, and enterprise settings. Interview participants included current and former officials from various organizations. Participants also included representatives from retail banks and current or former officials from other organizations.

To assess the potential of the proposed model's viability for transaction-processing design in supporting secure payments' needs and instant settlement preferences, the study identifies 12 critical success factors through semi-structured interviews conducted exclusively on experts from national, international, and private enterprises but excludes end-users to start with. The 12 critical success factors are aligned with the five categories of sustainable organizational performance of the balance scorecard: Finance, Customers, Internal business processes, Learning and growth, and Industry. The study analyzes these core decision-making issues using a qualitative process-protocol methodology. The resulting phase-based decision-making model serves as a repository to which a customizable template can be mapped for specific situations and organizational types that present different combinations of the decision-making issues. From a pragmatic perspective, the model serves as a ready reference for value creation initiatives to promote the strategic adoption of enterprise reporting and socially responsible organizational initiatives in the strategic direction of the installation.

3.3. Instant Settlement Networks

An Instant Settlement Network (ISN) is a financial network that facilitates instant settlement of payment and transfers among individual users, businesses, and government agencies. An ISN offers the same transaction model of a payment network but allows transferring value or credit between accounts of its users with instantaneous credit to the recipient's account. Payment networks only act as messaging networks for initiating transactions, with the actual transfer or settlement of funds taking hours or days. On the contrary, an ISN enables transfer and settlement to be done instantly at any time, even at nights and weekends when payment networks are closed or non-functioning. Today,

payment networks are not used for funds transfers due to their limitations. For international transactions, payment networks offer remittance services. Remittance transactions account for a small portion of the funds transfer transactions, compared to services provided by banks, credit card companies, and payment service providers. Remittance services using payment networks charge a high transaction fee to the sender for small value transactions.

An ISN also provides credit to borrowers and provides interest to depositors. It enables lenders and depositors to pair up with little or no expense and for small amounts. Offering instantaneous interest to depositors and to payers is the prime objective of the ISN. Market competition would drive the instantaneous interest for the depositors approaching zero. Consequently, an ISN facilitates periodical savings of small amounts or trading in securities using periodic installments. Other services offered by an ISN are tax collection, lottery settlements, property transfer, pension deposits, electoral fund transfers, and loans or insurance payments from the government.

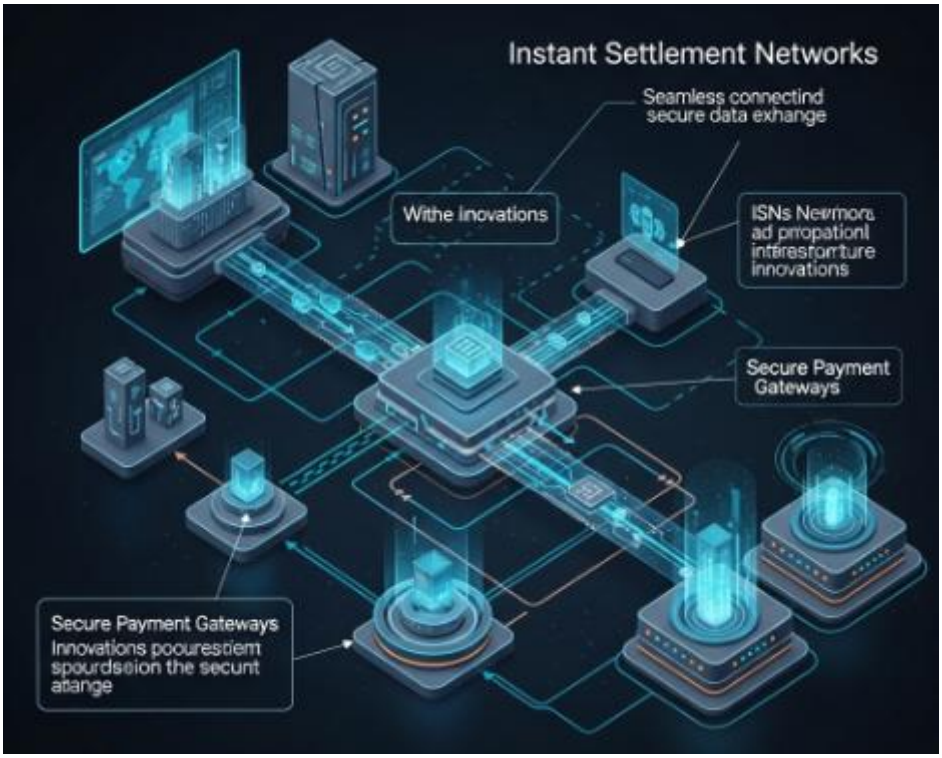

Fig 3.2: Instant Settlement Networks

3.3.1. Definition and Importance

Instant settlement networks are digital constructions of smart rules that organize and oversee the direct peer-to-peer transfer of value among network participants. These networks have a very limited settlement risk exposure window and, therefore, require very limited resources assigned to secure settlement and transfer of funds. Financial markets create value by providing liquidity. This liquidity is generated through the differential between bid and ask prices. The narrower the bid-ask differential and the more competitive the marketplace, the more liquidity and savings for the market participants. Even narrow market differentials present a considerable cost for payment systems when scaled for the number of payment transactions.

The instantaneous and secure transfer of funds found in instant settlement networks reduces the cost of capital for participants of financial systems, boosting market liquidity. This deep liquidity formation is especially helpful when the safety and integrity of the financial market come into question. An instant settlement network acts as a hard guarantee of transaction completion and finality even in extreme market conditions. In this case, the instant settlement network is an indispensable financial system service member behind payment gateways or transaction-based commerce systems. Settlement guarantees, alongside the instantaneous transfer of value, remove intermediaries whose only function has historically been to provide guarantees for the underlying transactions over long periods of time.

3.4. Secure Payment Gateways

Payment gateways securely process credit card payments for online businesses, bricks and mortar stores, and e-commerce sites. These service providers authorize the payment, ensuring that the customer has sufficient funds, and process it across the card networks. Payment gateways offer a variety of services, including fraud detection, which most online merchants rely upon to review potential chargebacks and fraudulent purchases. They are an essential channel through which consumers make billions of dollars in purchases every year.

To facilitate a credit card purchase, a customer provides their card number, cardholder name, expiration date, and card verification value (CVV) to a merchant. Depending on the merchant's processing arrangement, they may enter that information directly, or it may be sent from the checkout to their payment gateway. The information is stored temporarily in connection with a payment authorization. The data doesn't linger because consumer card data, especially CVV data, is extremely valuable and a target for hackers who want to sell it on the dark web. All payment gateways use encryption to make

encrypted payment authorizations over secure sockets layer and using the transaction approval process, or a corresponding protocol, of the card networks.

The payment gateways act on behalf of the acquirer processor during the approval process, notifying the acquirer processor of the final approval and forwarding the transaction's settlement information to initiate the transaction's deposit to the merchant's bank account. The transaction information is relayed back through the entire processing channel — to the bank that issued the payment card, to the merchant's acquirer processor, and back to the merchant. While a merchant must ultimately pay the fees of all parties in the transaction process chain, a payment gateway itself usually charges merchants a per-auth fee plus a daily or monthly minimum.

3.4.1. Overview of Payment Gateways

The evolution of electronic commerce has been made possible by the digitization of goods or services, leading to the creation of entirely new businesses and the radical transformation of their industries. Business use of the Internet includes banking, stock brokering, real estate, and commodity trading, where the immediacy of the Internet, and the availability of comparative data, drive transactions. Furthermore, the use of the Internet allows customers to find vendors for travel, entertainment, and other services. While mere advertisement by these vendors would have sufficed, the immediacy of the online transaction has led to the creation of a new business model, and accompanying requirements for intermediaries who can provide ease-of-access interfaces, and trusted transaction processing.

Such intermediary services of payment processing for e-commerce functions have sprung into existence. Acting as bridges between customers and merchant websites, they provide the functionality which helps authorize and post customer transactions to merchants' bank accounts. It is a prerequisite for companies wanting to engage in online payment processing to obtain a Merchant ID account from a bank. The process of payment processing has many stages, such as credit card transactions which start when a customer places his order online. The merchant website gets in touch with the payment gateway chosen by him for online payment only after confirming the availability of the goods or services he requires. The merchant then sends the credit card data for processing. The acquiring bank pays the respective merchant's bank once authorization is done. The information regarding sales authorization is sent to the merchant, and then he sends it to the payment gateway. The merchant is notified that the transaction has been completed by the gateway.

3.5. Architectural Innovations

Innovations in architecture allow older development stacks to be overcome, or new tools to be built, such that old development stacks are replaced by the new tools without damaging what's already built. For example, the development of a more secure protocol shifted developers from building gateway machines to simply applying it. In the space of instant settlement networks, allowing easier access to payment channels such that they become more broadly applied, less limited to merchants with loss-leader incentives; removing routing from L2, and allowing new L2 tools to be built that don't create asymmetric tax burdens for the L1 user are big architectural changes in open systems that will allow these systems to be more broadly applied.

Other ideas such as the balance proof have appeared from ZKPs, but not used as expense and as seamless as these channels offer. LD is a specialized payment channel; LN is not P2P symmetric because of the routing requirement; the L1 argument points to the band-aid that is L1-Payments to speed up withdrawals. The design overview thinks of this as eliminating third-party custodians, all L1 pens that force all lightning usage to be merchant payments because of how awful UX is. Furthermore, the chicken and egg problem of liquidity provisioning is partially mediated in L2 by cryptographic payment channel proofs, these proofs are pegged to the L1 network, thus creating an L2-L1 liquidity loop mechanism that encourages exchange.

3.5.1. Blockchain Technology

A significant challenge faced by secure gateway technologies is their management of trust and identity. Recent proposed innovations have exploited blockchain technologies to enable new trusted infrastructure that allows instant settlement of digital financial transactions without the counterparty risk otherwise created by a lack of trusted intermediary verification. Here, we review existing, architecturally enabled blockchain technology as it applies to the instant settlement of electronic commerce.

The general idea of blockchain technology is to securely enable authenticated and permissionless updates to databases without a centrally trusted third party. The first blockchain technology developed applied this idea in the domain of peer-to-peer electronic cash. In its design, physical cash is not transferable in the same way as traditional digital representations of value that are subject to payment systems that provide verification of counterparty's balances at the time of processing. The solution to the double spending problem was to create a global, permissionless database that contains a record of all transactions in a chain of hashes over time and is resistant to modification. This prevents the ability of malicious participants from inserting unsynchronized transactions into a validated transaction set, and creates a loss-back

mechanism whereby no set of transactions can be lost without also being lost in a greater valid transaction set. Since no party is trusted, invalid transaction checks and the accounting of valid transaction sets are done in a fully decentralized way. Since no party is permitted to add or modify transactions without the validation of the consensus process, cryptographically secure database tampering is impossible.

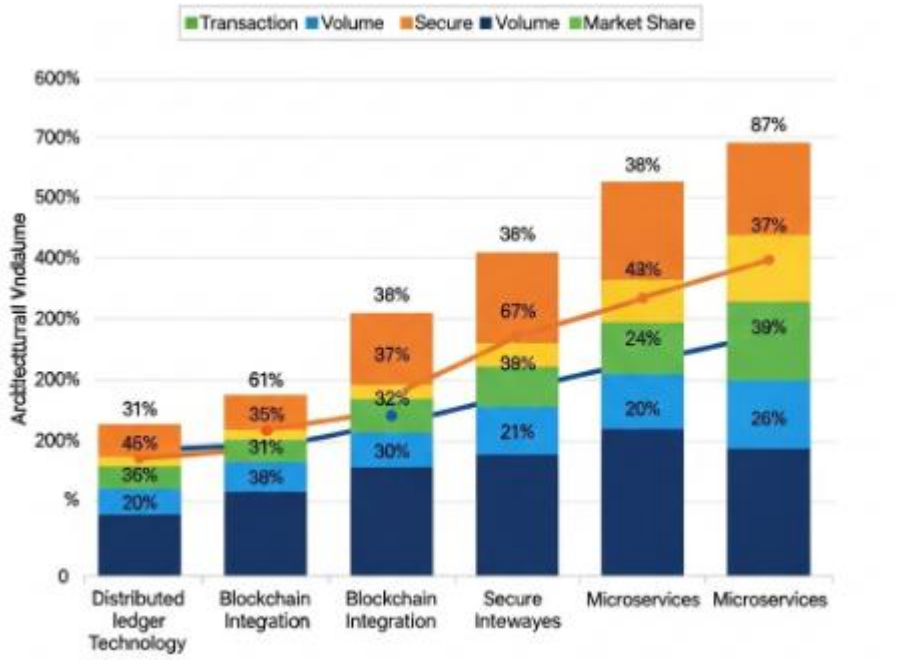

Fig : Instant Settlement Networks and Secure Payment Gateways

3.6. Integration of Instant Settlement and Secure Gateways

Integrating instant settlement and secure payment gateways enhances the trust in digital currency adoption for daily transactions. Cryptographic security formulations are often used to prevent double spending and reject illegitimate transactions. In legacy finance, chargebacks and reverse frauds on credit transactions deny the security offered by digital payment methods. Payment gateways verifying merchant identities and insuring payment amounts against payment method fraud on an integrated instant settlement network minimize related fraud. Instant settlement further improves the security of digital payments for the merchant and consumer by eliminating the indemnification wait for fraudulent transactions. The integration additionally allows the payment gateways to process transfers on the instant settlement network concurrently with other legacy payment methods. Merging digital currency payments with traditional card processing through the integrated payment gateway allows merchants to avoid needing point of sale or e-commerce modifications to accept digital currency for payment. The merchants

using enduring legacy processors do not need additional efforts to advertise and promote the availability of digital currency. Notifications via instant messaging or SMS are then sent to the merchants, their staff, and their customers that enable the digital currency to be used as a temporary incentive to market test digital payments. The additional overheads of multiple payment processors configured for delayed settlement, digital currency, and traditional card services is mitigated. Operations for finalizing payments after approval are streamlined for the merchant, cutting costs and saving time.

3.6.1. Benefits of Integration

Integrating instant settlement networks with secure payment gateways can offer several benefits, accelerating the adoption and enhancing the customer experience of digital payments further accelerating the shift to cashless economies. Through deep integrations, merchants offering digital payments as a method of offer settlement can get settlement within seconds of payment initiation while at the same time ensuring protection from settlement risk. Customers on the other hand are ensured secure payment initiation and completion experiences and are building ease of use confidence in digital payments for everyday transactions. Merchants can increase collections using integrated payment gateway approaches. Reduction in friction for the customer for funds that are either already there or can easily be there using an instant settlement solution ensures instant settlement of the merchants' accounts after order completion versus the vendor capturing the payment upfront and then releasing it after completion. Using instant settlement networks, settlement can happen minutes if not seconds after completion of the service or delivery of the goods. Thus, incremental volumes for vendors using Payment Gateways and integrated instant settlement networks should be significant, and they should definitely aim to do that.

3.7. Conclusion

Instant settlement networks facilitated by financial technology need innovative security architectures for the secure and efficient deployment of the channel networks for payment gateways. The conventional architectures underpinning these networks weigh a considerable burden on the core infrastructure, reducing the stress resistance and reliability of those environments mediating such payment gateways. This chapter examines such revolutionary designs with a view to solving the security challenges faced by instant settlement networks. The major concern of these networks and gateways not using block-based architectures online is to provide escrow-like conditions for simultaneously concerned users under zero latency. No latency exposes users to a large range of security attacks. Even though cybersecurity market research reports assume that

strengthening the cybersecurity of the Internet and the financial sector in particular will become among the biggest priorities, investments, and market trends of the decade, it is difficult to predict how the cybersecurity market will develop given the high volatility of certain segments of the market. Cybersecurity is a long-run trend. All abundant predictions show that cybersecurity issues will create a turning point in the development of IT solutions for small businesses and financial institutions in particular, given the historical-discursive context in cyberspace security debates and how this will impact existing solutions. The same upheaval can be seen in the cybersecurity market, moving away from focusing on defending computing resources belonging to a single organization or person from hackers toward protecting the cyberspace associated with securitization of space and transactions.

3.7.1. Emerging Trends

Digital payment systems have evolved over the past decades owing to the trend of decentralized systems. Recent years have seen the growth of interest in new products and services in the arena of closed and open-loop instant payment systems. A recent appointment of a dedicated team of experts in instant payment systems indicates the significance attached to this emerging technological trend in shaping the future of payment systems and settlement risk in monetary policy.

Central banks are focusing on new potential threats to Public Service Wholesale Aspects. A declaration highlights the importance of access to New Payment Services for central banks. Developers are exploring the creation of full-fledged Central Bank Digital Currency for interbank settlement purposes operating on Traditional Interbank Payment Systems. However, digital currencies for interbank payment settlement are yet to become a commercial reality. Prototypes of digital currency wallets have been developed but are not yet embedded in infrastructure.

One of the key monetary policy objectives is to preserve financial stability. A study reveals that a digital currency operating system could lower the effective lower bound on interest rates, easing the conduct of monetary policy, while a proposal suggests a monetary policy chart. The Treasury Department is working on improvements to the existing Interbank Payment System based on TIPS. However, the first mobile wallets and instant payment products have not yet been launched or fully deployed. A report has proposed a framework for the implementation of a payment system. A next generation Digital Payment and Settlement Network Framework consists of detection and neutralization bots. These bots are embedded in the architecture to detect, intercept and neutralize threats to digital services operating on the framework.

References

Malempati, M. (2024). Leveraging cloud computing architectures to enhance scalability and security in modern financial services and payment infrastructure. European Advanced Journal for Science & Engineering (EAJSE)-p-ISSN 3050-9696 en e-ISSN 3050-970X, 2(1).

Mwale, M., & Phiri, J. (2024, February). Secure Mobile Payment Gateway for Higher Institutions of Learning. In International Congress on Information and Communication Technology (pp. 367-381). Singapore: Springer Nature Singapore.

Bojjagani, S., Sastry, V. N., Chen, C. M., Kumari, S., & Khan, M. K. (2023). Systematic survey of mobile payments, protocols, and security infrastructure. Journal of Ambient Intelligence and Humanized Computing, 14(1), 609-654.

Carstens, A. G., & Nilekani, N. (2024). Finternet: the financial system for the future (pp. 1-38). Basel: Bank for International Settlements, Monetary and Economic Department.

Hefny, M. H. M., Helmy, Y., & Abdelsalam, M. (2023). Open banking api framework to improve the online transaction between local banks in egypt using blockchain technology. Journal of Advances in Information Technology, 14(4), 729-740.