E- PAYMENTS SYSTEM

BBA
Semester-V

Lesson Writers

Lesson Writer & Editor
Dr. Nagaraju Battu
Associate Professor
Dept. of MBA (HRM)
Acharaya Nagarjuna University

Dr. B. Sreedhar Reddy
Faculty
Dept. of MBA (Hospital Administration)
Acharaya Nagarjuna University

Dr. K. Sudheer Kumar
Faculty
Dept. of Commerce & Buss. Admin.
Acharaya Nagarjuna University

Dr. Ch. Prasad
Faculty
Dept. of MBA (Hospital Administration)
Acharaya Nagarjuna University

Director

Dr. NAGARAJU BATTU
MBA., MHRM., LLM., M.Sc. (Psy).,MA (Soc)., M.Ed., M.Phil., Ph.D

CENTRE FOR DISTANCE EDUCATION

ACHARAYA NAGARJUNA UNIVERSITY

NAGARJUNA NAGAR – 522 510
Ph: 0863-2293299, 2293214,
Website: www.anucde.info
e-mail:anucdedirector@gmail.com

BBA: E- PAYMENTS SYSTEM

First Edition: 2024

No. of Copies :

This book is exclusively prepared for the use of students BBA Centre for Distance Education, Acharya Nagarjuna University and this book is meant for limited circulation only.

Published by:
Dr. NAGARAJU BATTU,
Director
Centre for Distance Education,
Acharya Nagarjuna University

Printed at:

FOREWORD

Since its establishment in 1976, Acharya Nagarjuna University has been forging ahead in the path of progress and dynamism, offering a variety of courses and research contributions. I am extremely happy that by gaining 'A' grade from the NAAC in the year 2016, Acharya Nagarjuna University is offering educational opportunities at the UG, PG levels apart from research degrees to students from over 443 affiliated colleges spread over the two districts of Guntur and Prakasam.

The University has also started the Centre for Distance Education in 2003-04 with the aim of taking higher education to the door step of all the sectors of the society. The centre will be a great help to those who cannot join in colleges, those who cannot afford the exorbitant fees as regular students, and even to housewives desirous of pursuing higher studies. Acharya Nagarjuna University has started offering B.A., and B.Com courses at the Degree level and M.A., M.Com., M.Sc., M.B.A., and L.L.M., courses at the PG level from the academic year 2003-2004 onwards.

To facilitate easier understanding by students studying through the distance mode, these self-instruction materials have been prepared by eminent and experienced teachers. The lessons have been drafted with great care and expertise in the stipulated time by these teachers. Constructive ideas and scholarly suggestions are welcome from students and teachers involved respectively. Such ideas will be incorporated for the greater efficacy ofthis distance mode of education. For clarification of doubts and feedback, weekly classes and contact classes will be arranged at the UG and PG levels respectively.

It is my aim that students getting higher education through the Centre for Distance Education should improve their qualification, have better employment opportunities andin turn be part of country's progress. It is my fond desire that in the years to come, the Centre for Distance Education will go from strength to strength in the form of new courses and by catering to larger number of people. My congratulations to all the Directors, Academic Coordinators, Editors and Lesson- writers of the Centre who have helped in these endeavors.

Prof. Raja Sekhar Patteti
Vice-Chancellor
Acharya Nagarjuna University

B.B.A -Semester – V
506BBE21- e-Payments System

Unit-I:

e-Cash and Virtual Money:Electronic Data Interchange (EDI) -NEFT/RTGS/Electronic Payment modes - Foundations of e-Cash and Issues; Security, Anonymity, Untraceability, Virtual currencies, Bitcoin.

Unit-II:

Automated Clearing and Settlement: Process ofReal Time Gross Settlement System - Net Settlement - ATM Networks - Fedwire, CHIPS and SWIFT.

Unit-III:

e-Payment Security and Digital Signature: Cryptographic Methods - Hash functions - Public/Private Key methods: RSA - Digital Signatures - Certification Process - Digital identity Documents and Remote Authentication.

Unit-IV:

Mobile Payments:Wireless payments, Digital Wallets, Google Wallet – Obopay - Security Challenges – Debit & Credit Cards – RU Pay Card – e-Challan.

Unit-V:

Electronic Invoice and Payment System:Electronic Statement Delivery - EIPP providers - Biller service providers - Customer service providers - Reconciliation through Bank -Invoice Paper elimination - Scan-based trading (SBT).

References:

1. Domonique Rambure and Alec Nacamuli, "Payment Systems: From the Salt Mines to the Board Room", Palgrave MacMillan.

2. WeidongKou, *"Payment Technologies for E-Commerce"*. Springer, Germany.

3. DonalO'Mahony, Michael Peirce and Hitesh Tewari, "Electronic Payment Systems", Artech House, Inc.

4. M. H. Sherif, Protocols for Secure Electronic Commerce, Boca Raton, Fla, CRC Press.

(506BBE21)

MODEL QUESTION PAPER

B.B.A. DEGREE EXAMINATION,

Third Year – Fifth Semester

Part II

Paper VI – E–PAYMENTS SYSTEM

Time : Three hours **Max. Marks: 70**

SECTION A–(5 x 4 = 20 marks)

Answer any FIVE of the following.

Each question carries 4 marks.

1. Virtual Money.

2. EDI.

3. Fedwire.

4. Remote Authentication.

5. E–challan.

6. Digital Wallets.

7. Electronic Invoice.

8. SBT.

SECTION B – (5 x 10 = 50 marks)

Answer ALL questions.

Each question carries 10 marks.

9. (a) What is NEFT and explain the reasons for NETT failure.

Or

(b) What is e–cash and explain major components of e–cash.

10. (a) What is Real time governance and explain the objectives of real time governance system.

Or

(b) Write about Net settlements and Gross settlement.

11. (a) Explain the advantages and limitations of digital signature.

Or

(b) Explain the differences between remote authentication and local authentication.

12. (a) Explain the advantages and limitations of Credit Cards.

Or

(b) Explain various security challenges in mobile payments.

13. (a) Describe about EIPP providers in detail.

Or

(b) What is Reconciliation and explain the steps involved in Bank Reconciliation.

CONTENTS

Lesson- 1
INTRODUCTION TO E-CASH AND VIRTUAL MONEY

Learning Objectives

- To Define electronic cash (e-cash) and virtual money, distinguishing between the two concepts.
- To Explain the characteristics and features of e-cash and virtual money, including decentralization, security, and borderless transactions.
- To Discuss the advantages and challenges associated with the use of e-cash and virtual money in financial transactions.
- To Analyze the impact of e-cash and virtual money on financial inclusion, innovation in payment systems, and economic growth.
- To Engage in critical thinking about the societal and economic implications of widespread adoption of e-cash and virtual money.

Structure

1.0 Introduction

Electronic cash, or e-cash, refers to digital money that enables secure and convenient online transactions. For MBA students, understanding e-cash is crucial as it plays a significant role in modern finance and digital economies.

Definition: E-cash, also known as digital currency or electronic money, is a form of currency that exists only in digital form. It allows for secure and instant transactions over the internet without the need for physical currency.

1.1 The History of e-Cash

1. Early Concepts (1970s-1980s):

- The idea of electronic cash began to emerge in the 1970s and 1980s with the rise of digital technologies and the increasing use of computers in financial transactions.
- Innovators and researchers started exploring ways to facilitate secure electronic transactions without the need for physical currency or traditional banking systems.

2. David Chaum and DigiCash (1980s-1990s):

- David Chaum, an American cryptographer, is often credited as one of the pioneers of digital cash. In the late 1980s, he developed the concept of blinded signatures, a cryptographic technique that allows for secure and anonymous transactions.
- In 1990, Chaum founded DigiCash, a company aimed at implementing his vision of electronic cash. DigiCash introduced "e-Cash," a digital currency that provided privacy and security through cryptographic techniques.
- Despite early promise, DigiCash struggled to gain widespread adoption due to regulatory challenges, lack of infrastructure, and competition from traditional payment systems.

3. Emergence of Online Payment Systems (1990s):

- In the 1990s, as the internet gained popularity, various online payment systems emerged to facilitate electronic transactions. Companies like PayPal (founded in 1998) and CyberCash (founded in 1994) offered digital payment solutions, but they primarily relied on traditional banking infrastructure rather than true electronic cash.

4. Bitcoin and Cryptocurrencies (2000s-present):

- The breakthrough moment for electronic cash came with the introduction of Bitcoin in 2009 by an unknown person or group using the pseudonym Satoshi Nakamoto. Bitcoin introduced the concept of a decentralized digital currency based on blockchain technology.
- Blockchain, a distributed ledger technology, allows for secure, transparent, and decentralized transactions without the need for intermediaries like banks. Bitcoin's innovation lies in its ability to achieve consensus among network participants without a central authority.
- Following Bitcoin's success, numerous alternative cryptocurrencies (altcoins) emerged, each with its unique features and use cases. Examples include Ethereum, Litecoin, Ripple, and many others.

5. Central Bank Digital Currencies (CBDCs) (2010s-present):

- In recent years, central banks worldwide have shown increasing interest in issuing their digital currencies, known as central bank digital currencies (CBDCs). CBDCs aim to combine the advantages of digital cash with the stability and trust associated with fiat currencies issued by central authorities.
- Several countries, including China, Sweden, and the Bahamas, have already conducted pilots or announced plans to launch CBDCs. The emergence of CBDCs represents a significant evolution in the history of electronic cash and has the potential to reshape the global financial system.

6. Current Landscape:

- Today, e-cash encompasses a diverse range of digital payment methods, including cryptocurrencies, mobile wallets, contactless payments, and central bank digital currencies.
- E-cash continues to evolve rapidly, driven by advancements in technology, changing consumer preferences, and regulatory developments. It plays a crucial role in the digital economy, enabling secure, efficient, and convenient financial transactions across the globe.

1.2 Overview of E-cash

1.2.1Types of E-cash

Centralized: These are digital currencies issued and regulated by a central authority, such as a government or a financial institution. Examples include digital versions of national currencies issued by central banks.

Decentralized: Decentralized e-cash operates on blockchain technology, where transactions are recorded on a distributed ledger without the need for a central authority. The most famous example is Bitcoin, but there are many other cryptocurrencies like Ethereum, Litecoin, etc.

Stored-Value Cards: These are prepaid cards with a specific monetary value stored electronically. They can be used for purchases at specific merchants or for general transactions.

1.2.2 Features of E-cash

Security: E-cash transactions are secured through encryption techniques, making them difficult to counterfeit or manipulate.

Anonymity: Depending on the system, e-cash transactions can offer varying degrees of anonymity, which can be advantageous for privacy-conscious users.

Accessibility: E-cash facilitates transactions across geographical boundaries, enabling seamless international trade and financial transactions.

Speed: Digital transactions are processed much faster than traditional banking methods, allowing for near-instantaneous transfers of funds.

1.2.3 Advantages

Convenience: E-cash transactions can be conducted anytime, anywhere, as long as there's an internet connection.

Lower Transaction Costs: Compared to traditional banking systems, e-cash transactions often incur lower fees.

Global Reach: E-cash facilitates cross-border transactions without the need for currency exchange, reducing complexities and costs associated with international trade.

1.2.4 Challenges

Security Concerns: E-cash systems are susceptible to hacking, fraud, and other cybersecurity threats.

Regulatory Challenges: Governments and regulatory bodies are still grappling with how to regulate e-cash effectively, leading to uncertainty and potential legal issues.

Volatility: Some digital currencies experience significant price fluctuations, posing risks to users and investors.

1.2.5 Applications

Online Payments: E-cash is widely used for online shopping, bill payments, and other digital transactions.

Remittances: It facilitates fast and cost-effective cross-border remittances, particularly for migrant workers sending money back to their home countries.

Smart Contracts: Decentralized e-cash platforms like Ethereum enable the execution of smart contracts, which are self-executing contracts with the terms of the agreement directly written into code.

1.2.6 Future Trends

Central Bank Digital Currencies (CBDCs): Several countries are exploring the development of CBDCs, which could potentially reshape the landscape of e-cash by providing a digital version of fiat currency.

Integration with Emerging Technologies: E-cash is likely to integrate with emerging technologies like artificial intelligence, Internet of Things (IoT), and blockchain to offer more sophisticated and efficient financial solutions.

1.3 Emergence of Virtual Currencies

The emergence of virtual currencies represents a significant milestone in the evolution of digital finance and the global economy. While the concept of digital currencies dates back to the early days of the internet, the true breakthrough came with the introduction of Bitcoin in 2009.

Bitcoin, created by an unknown person or group using the pseudonym Satoshi Nakamoto, was the first decentralized cryptocurrency. It introduced a revolutionary concept: a peer-to-peer electronic cash system that operates without the need for intermediaries like banks or central authorities. Bitcoin's underlying technology, known as blockchain, provided a decentralized and secure way to record transactions and maintain a transparent ledger.

The release of Bitcoin whitepaper in October 2008 was a precursor to its launch in January 2009, marking the beginning of the virtual currency era. Bitcoin's decentralized nature, cryptographic security, and limited supply (capped at 21 million coins) attracted early adopters, technologists, libertarians, and investors intrigued by the potential of digital currencies to disrupt traditional financial systems.

Following Bitcoin's success, numerous alternative cryptocurrencies, or altcoins, emerged, each with its unique features and use cases. Ethereum, launched in 2015, introduced smart contract functionality, enabling developers to create decentralized applications (DApps) and programmable digital assets. Litecoin, launched in 2011, aimed to improve upon Bitcoin's transaction speed and scalability.

The emergence of virtual currencies facilitated the rise of a vibrant and diverse ecosystem encompassing exchanges, wallets, mining operations, and blockchain startups. Cryptocurrencies gained traction as a speculative investment, a medium of exchange for online transactions, and a hedge against traditional financial instruments.

While virtual currencies offer exciting opportunities for innovation and financial inclusion, they also pose challenges and risks. Price volatility, regulatory uncertainty, security vulnerabilities, and concerns about illicit activities have been ongoing issues in the cryptocurrency space. Despite these challenges, virtual currencies continue to attract attention and investment from individuals, institutions, and governments worldwide.

In recent years, the concept of central bank digital currencies (CBDCs) has gained prominence, with several countries exploring the possibility of issuing their digital currencies. CBDCs aim to combine the benefits of digital currency with the stability and trust associated with fiat currencies issued by central banks. The emergence of CBDCs represents a significant development in the evolution of virtual currencies and has the potential to reshape the global financial landscape.

Overall, the emergence of virtual currencies represents a paradigm shift in the way we think about money, value exchange, and financial systems. As technology continues to evolve and societal attitudes toward digital currencies evolve, virtual currencies are likely to play an increasingly prominent role in the future of finance.

1.4 Overviewof Virtual Currencies

Definition: Virtual currencies are digital or virtual representations of value that are not issued or regulated by any central authority. They operate on decentralized networks, typically based on blockchain technology, which allows for peer-to-peer transactions without the need for intermediaries.

Decentralization: Virtual currencies, such as Bitcoin, Ethereum, and Litecoin, operate on decentralized networks, where transactions are verified and recorded by a distributed network of nodes. There is no central authority controlling the issuance or circulation of virtual currencies.

Regulation: Virtual currencies operate in a relatively unregulated environment, although governments and regulatory bodies have begun to introduce measures to address concerns such as money laundering, tax evasion, and consumer protection. Regulations vary significantly by country and jurisdiction.

Examples: Examples of virtual currencies include Bitcoin, Ethereum, Ripple, and other cryptocurrencies, as well as in-game currencies used in virtual worlds and online gaming platforms.

1.5 The Scope of Virtual Currency

1. Financial Inclusion: Virtual currencies have the potential to increase financial inclusion by providing access to financial services for individuals who are unbanked or underbanked. Through virtual currencies, people can participate in the global economy, transfer funds, and store value without the need for traditional banking infrastructure.

2. Cross-Border Payments: Virtual currencies facilitate fast and cost-effective cross-border payments. They eliminate the need for intermediaries, such as banks and remittance companies, reducing transaction fees and processing times. This can benefit individuals sending remittances to their home countries and businesses engaged in international trade.

3. Decentralized Finance (DeFi): Virtual currencies are central to the growth of decentralized finance (DeFi) ecosystems. DeFi platforms leverage blockchain technology and smart contracts to offer financial services such as lending, borrowing, trading, and yield farming without intermediaries. DeFi has the potential to democratize access to financial services and create new opportunities for global financial inclusion.

4. Investment and Speculation: Virtual currencies serve as investment assets and speculative instruments for individuals, institutions, and traders. The volatile nature of virtual currency markets offers opportunities for profit but also carries risks. Investors may hold virtual currencies as part of their diversified investment portfolios or engage in trading for short-term gains.

5. Blockchain Technology: Virtual currencies drive innovation in blockchain technology, the underlying technology that enables secure and transparent transactions. Blockchain has applications beyond virtual currencies, including supply chain management, digital identity, voting systems, and more. Virtual currencies serve as a catalyst for blockchain development and adoption.

6. Regulatory Landscape: The scope of virtual currency is influenced by regulatory frameworks established by governments and regulatory bodies worldwide. Regulatory approaches vary by jurisdiction, with some countries embracing virtual currencies, while others impose restrictions or bans. Regulatory clarity and compliance play a significant role in shaping the future of virtual currencies.

7. Consumer Adoption and Education: As virtual currencies continue to gain mainstream attention, consumer adoption and education become crucial. Understanding the risks and benefits of virtual currencies, as well as how to securely store and transact with them, is essential for widespread adoption. Education initiatives, user-friendly interfaces, and regulatory safeguards can promote responsible use of virtual currencies.

8. Central Bank Digital Currencies (CBDCs): The scope of virtual currency includes the emergence of central bank digital currencies (CBDCs). CBDCs are digital representations of fiat currencies issued by central banks. They aim to combine the benefits of virtual currencies with the stability and trust associated with traditional fiat currencies. CBDCs have the potential to reshape the global monetary system and enhance financial inclusion.

1.6 Impact of e-cash and virtual money on financial inclusion, innovation in payment systems, and economic growth

The emergence of e-cash and virtual money has profoundly influenced financial inclusion, innovation in payment systems, and economic growth. In terms of financial inclusion, these digital currencies have extended the reach of financial services to previously underserved populations, such as those in remote areas or without access to traditional banking infrastructure. By facilitating easier and more accessible transactions, e-cash and virtual money have enabled individuals to participate more fully in the formal financial system, thus promoting greater economic inclusivity.

Moreover, the innovation spurred by these digital currencies has revolutionized payment systems, introducing faster, cheaper, and more secure methods of transferring funds. Traditional banking systems often involve lengthy processes and high transaction fees, particularly for cross-border transactions. However, e-cash and virtual money have streamlined these processes, offering near-instantaneous transactions at lower costs. This has not only enhanced efficiency within financial systems but has also fostered greater convenience and accessibility for users worldwide.

Furthermore, the adoption of e-cash and virtual money has contributed to economic growth by stimulating various sectors and promoting entrepreneurship. The increased ease of conducting financial transactions has encouraged the development of new businesses, particularly in the digital realm. Additionally, the reduced barriers to entry for financial services have empowered individuals to engage in economic activities, such as investing, saving, and purchasing goods and services. As a result, the broader accessibility and efficiency of financial transactions facilitated by e-cash and virtual money have played a significant role in driving economic expansion and prosperity.

1.7 Societal and economic implications of widespread adoption of e-cash and virtual money

The widespread adoption of e-cash and virtual money carries significant societal and economic implications. On a societal level, it has the potential to reshape the way individuals interact with money and financial services. The convenience and accessibility offered by digital currencies can empower individuals, particularly those in underserved communities, by providing them with access to banking services and enabling them to participate more fully in the formal economy. However, it also raises concerns about digital divides and cybersecurity risks, as not everyone may have equal access to or understanding of these technologies, and the prevalence of online transactions may expose users to potential fraud or data breaches.

From an economic standpoint, the adoption of e-cash and virtual money has the potential to enhance efficiency and drive innovation in payment systems. By streamlining transactions and reducing transaction costs, digital currencies can facilitate faster and cheaper exchange of goods and services, thus promoting economic growth. Additionally, the emergence of blockchain technology, which underpins many digital currencies, has the potential to revolutionize various industries beyond finance, such as supply chain management, healthcare, and voting systems. However, regulatory challenges and concerns about financial stability and monetary policy may arise as digital currencies become more prevalent, requiring careful consideration and adaptation of regulatory frameworks to ensure stability and consumer protection in the evolving financial landscape.

1.8 Summary

In this introductory lesson on e-cash and virtual money, we explore the fundamental concepts, characteristics, and implications of digital currencies in the modern financial landscape. E-cash, as a form of electronic currency, and virtual money, encompassing cryptocurrencies and in-game currencies, offer decentralized, secure, and borderless transactions, revolutionizing traditional banking systems. While these currencies promise increased accessibility and reduced transaction costs, they also present challenges such as regulatory uncertainty and susceptibility to cyber threats. Nonetheless, their emergence fosters financial inclusion, innovation in payment systems, and economic growth, urging stakeholders to adapt to the evolving dynamics of digital finance while balancing innovation with risk management.

1.9 Keywords

E-Cash: Electronic cash, or e-cash, refers to digital money that enables secure and convenient online transactions.

Anonymity: Depending on the system, e-cash transactions can offer varying degrees of anonymity, which can be advantageous for privacy-conscious users.

Accessibility: E-cash facilitates transactions across geographical boundaries, enabling seamless international trade and financial transactions.

Remittances: It facilitates fast and cost-effective cross-border remittances, particularly for migrant workers sending money back to their home countries.

Volatility: Some digital currencies experience significant price fluctuations, posing risks to users and investors.

1.10 Self-Assessment Questions

1. What is e-cash, and how does it differ from traditional physical currency?
2. Describe the characteristics of virtual money, providing examples of virtual currencies.
3. What are the advantages of using e-cash and virtual money in financial transactions?
4. Identify two challenges associated with the widespread adoption of e-cash and virtual money.
5. How do e-cash and virtual money contribute to financial inclusion?
6. Explain the concept of decentralization in the context of digital currencies.
7. What role does cryptography play in securing e-cash and virtual money transactions?
8. Discuss one potential application of virtual money outside of financial transactions.
9. How might regulatory frameworks impact the adoption and use of e-cash and virtual money?
10. Reflect on the future trends and considerations for e-cash and virtual money, considering factors such as technological advancements and regulatory changes.

1.11 Suggested Readings

1. Finn Brunton (2019). "Digital Cash: The Unknown History of the Anarchists, Utopians, and Technologists Who Created Cryptocurrency", Princeton University Press.
2. Paul Vigna and Michael J. Casey (2016). "The Age of Cryptocurrency: How Bitcoin and Digital Money Are Challenging the Global Economic Order", St. Martin's Press.
3. Daniel Drescher (2017). "Blockchain Basics: A Non-Technical Introduction in 25 Steps", Apress.
4. Saifedean Ammous (2018). "The Bitcoin Standard: The Decentralized Alternative to Central Banking", Wiley Publications.
5. Paul Vigna and Michael J. Casey (2015). "Cryptocurrency: How Bitcoin and Digital Money are Challenging the Global Economic Order", St. Martin's Press
6. Andreas M. Antonopoulos (2017). "Mastering Bitcoin: Unlocking Digital Cryptocurrencies", O'Reilly Media.

Dr. Nagaraju Battu

Lesson- 2
PAYMENT MODES: NEFT AND RTGS IN ELECTRONIC DATA INTERCHANGE

Learning Objectives

- To Understand the Concepts of NEFT, and RTGS payment modes
- To Explore Operational Processes from initiating to completing transactions in EDI, NEFT, and RTGS.
- To Evaluate the suitability of each mode for different types of transactions, considering factors such as transaction speed, cost, and transaction limits.

Structure

2.0 Introduction

Electronic Data Interchange (EDI) is a standardized method for businesses to exchange documents electronically, offering benefits such as cost reduction, efficiency, and improved accuracy. However, implementing and managing EDI systems comes with challenges, including complexity and security concerns. Looking ahead, emerging trends such as cloud-based solutions, AI integration, and blockchain technology are poised to shape the future of EDI.

2.1 Electronic Data Interchange (EDI)

Definition: EDI is the computer-to-computer exchange of business documents in a structured, machine-readable format. It enables companies to exchange documents such as purchase orders, invoices, shipping notices, and other business documents without human intervention.

Standardization: One of the key aspects of EDI is standardization. Standard formats, such as ANSI X12, EDIFACT, and XML, are used to ensure compatibility and interoperability between different systems. These standards define the structure and content of the documents being exchanged.

2.1.1 Benefits

Cost Reduction: By automating document exchange processes, companies can reduce the costs associated with manual handling, printing, mailing, and data entry.

Efficiency: EDI speeds up the exchange of documents, reducing the time it takes to process transactions and improving overall efficiency.

Accuracy: Manual data entry is prone to errors, but EDI minimizes these errors by automating the process, leading to higher data accuracy.

Improved Relationships: EDI fosters better relationships between trading partners by providing real-time visibility into transactions and improving communication.

Compliance: Many industries have regulatory requirements for document exchange. EDI helps companies comply with these regulations by ensuring that documents are exchanged according to the specified standards.

2.1.2 Components

Translation Software: Converts business documents into the appropriate EDI format for transmission and vice versa.

Communication Protocol: Determines how data is transmitted between trading partners, commonly using protocols like AS2 (Applicability Statement 2), FTP (File Transfer Protocol), or VANs (Value-Added Networks).

Data Mapping: Maps data fields from internal systems to the corresponding fields in the EDI standard format.

EDI Standards: Specifies the structure and format of documents exchanged, ensuring consistency and compatibility across different systems.

Integration: EDI systems often need to integrate with internal systems such as ERP (Enterprise Resource Planning) or accounting software.

2.1.3 Process

Document Generation: Business documents are generated in the company's internal system.

Translation: The documents are translated into the EDI format using translation software.

Transmission: The EDI documents are transmitted to the trading partner using the agreed-upon communication protocol.

Receipt and Translation: The trading partner receives the documents, translates them back into their internal format, and processes them accordingly.

2.1.4 Challenges:

Implementation Costs: Setting up EDI systems can require significant initial investment in software, hardware, and training.

Complexity: Implementing and managing EDI systems can be complex, especially for smaller businesses with limited resources.

Trading Partner Requirements: Different trading partners may have different EDI requirements, leading to additional complexity in implementation and maintenance.

Security Concerns: Transmitting sensitive business data electronically raises security concerns. Implementing secure communication protocols and encryption is essential to mitigate these risks.

2.1.5 Future Trends:

Cloud-Based Solutions: Cloud-based EDI solutions are becoming more popular, offering scalability, flexibility, and reduced maintenance overhead.

Integration with AI and Automation: Integration with artificial intelligence (AI) and robotic process automation (RPA) technologies can further streamline EDI processes and improve efficiency.

Blockchain Integration: Blockchain technology has the potential to enhance the security and traceability of EDI transactions by providing a tamper-resistant and transparent ledger of transactions.

2.2 Electronic Payment Modes

Electronic payment modes offer convenient, fast, and secure ways to transfer funds electronically, with various options available to consumers and businesses. While they offer numerous benefits, electronic payments also pose risks and challenges related to security, privacy, and regulatory compliance. Looking ahead, emerging trends such as contactless payments, biometric authentication, and CBDCs are expected to shape the future of electronic payments.

Definition: Electronic payment modes involve the transfer of funds electronically, often through banking systems or online platforms, without the need for physical cash or checks.

2.2.1 Types of Electronic Payment Modes

Credit and Debit Cards: These are among the most widely used electronic payment methods, allowing consumers to make purchases by swiping or inserting cards at point-of-sale terminals or entering card information online.

Online Banking: This involves using online banking platforms to transfer funds between accounts, pay bills, or make purchases online.

Mobile Payments: Mobile payment apps enable users to make payments using their smartphones or other mobile devices. Examples include Apple Pay, Google Pay, and Samsung Pay.

Digital Wallets: Digital wallets store payment information securely and can be used to make payments in-store, online, or via mobile devices. Examples include PayPal, Venmo, and Cash App.

ACH Transfers: Automated Clearing House (ACH) transfers enable bank-to-bank transfers of funds, often used for direct deposits, bill payments, and business-to-business transactions.

Cryptocurrencies: Cryptocurrencies like Bitcoin and Ethereum facilitate peer-to-peer electronic payments using blockchain technology.

Electronic Funds Transfer (EFT): EFT involves the electronic transfer of funds between bank accounts, often used for payroll deposits, recurring bill payments, and large transactions.

2.2.2 Benefits

Convenience: Electronic payment modes offer greater convenience compared to traditional payment methods like cash or checks, allowing for quick and easy transactions.

Speed: Transactions can be processed almost instantly, reducing the time it takes for funds to transfer between parties.

Security: Electronic payment systems employ various security measures such as encryption, tokenization, and multi-factor authentication to protect sensitive financial information.

Record-Keeping: Electronic payments generate digital records of transactions, making it easier to track spending, reconcile accounts, and maintain financial records.

Accessibility: Electronic payment modes are accessible 24/7 from anywhere with an internet connection, providing greater flexibility for users.

2.2.3 Risks and Challenges

Security Concerns: Despite security measures, electronic payment systems are vulnerable to hacking, fraud, and data breaches.

Privacy Issues: Electronic payments may involve sharing personal and financial information with third parties, raising concerns about privacy and data protection.

Technical Issues: System outages, software glitches, and connectivity issues can disrupt electronic payment services, impacting users and businesses.

Regulatory Compliance: Electronic payment providers must comply with regulations related to data security, consumer protection, and anti-money laundering, adding complexity to operations.

Costs: While electronic payments can be cost-effective for consumers and businesses, fees may apply for certain transactions, especially cross-border payments or expedited transfers.

2.2.4 Future Trends

Contactless Payments: Contactless payment methods, such as NFC-enabled cards and mobile wallets, are growing in popularity due to their convenience and hygienic benefits.

Biometric Authentication: Biometric technologies like fingerprint scanning and facial recognition are increasingly being used to enhance security and streamline authentication for electronic payments.

Embedded Payments: Payments integrated into Internet of Things (IoT) devices, smart appliances, and wearable devices enable seamless transactions as part of everyday activities.

Central Bank Digital Currencies (CBDCs): Some governments are exploring the issuance of digital currencies backed by central banks, which could revolutionize electronic payments and monetary systems.

Enhanced Security Measures: Continuous advancements in encryption, tokenization, and fraud detection technologies will continue to improve the security of electronic payment systems.

2.3 Real-Time Gross Settlement (RTGS)

Real-Time Gross Settlement (RTGS) is a payment mode used for immediate and irrevocable settlement of high-value transactions. It offers benefits such as speed, finality, and liquidity management, but may also incur higher fees compared to other payment modes. Regulatory oversight and ongoing technological advancements are expected to shape the future of RTGS systems, enhancing efficiency, interoperability, and security in the global financial ecosystem.

Definition: RTGS is a funds transfer system where the transfer of money or securities takes place from one bank to another on a "real-time" and "gross" basis. Real-time means the transaction is processed immediately and gross settlement means each transaction is settled individually, without netting with other transactions.

2.3.1 Key Features:

Immediate Settlement: RTGS transactions are settled instantly, providing immediate availability of funds to the recipient.

High-Value Transactions: RTGS is primarily used for high-value transactions that require immediate and irrevocable settlement, such as interbank transfers, large corporate payments, and government securities transactions.

No Transaction Limit: Unlike some other payment modes, RTGS typically does not have a maximum transaction limit, allowing for the transfer of large sums of money.

Centralized System: RTGS systems are usually operated by central banks or monetary authorities to facilitate secure and efficient high-value transactions.

2.3.2 Process:

Initiation: The sender initiates an RTGS transaction through their bank, providing details such as the recipient's account number, the amount to be transferred, and any additional information required for processing.

Authorization: The sender's bank verifies the transaction details and authorizes the transfer of funds, debiting the sender's account.

Settlement: The transaction is then routed through the RTGS system, where it is settled in real-time by transferring funds from the sender's bank to the recipient's bank.
Confirmation: Once the funds are successfully transferred, both the sender and the recipient receive confirmation of the transaction.

2.3.3 Operating Hours:

- RTGS systems typically operate during predefined hours, which may vary depending on the jurisdiction and the central bank's policies.
- Some RTGS systems operate on a 24/7 basis to accommodate global financial markets and facilitate cross-border transactions across different time zones.

2.3.4 Benefits:

Speed: RTGS enables immediate settlement of high-value transactions, providing fast and efficient fund transfers.
Finality: Transactions settled through RTGS are irrevocable and final, reducing counterparty risk for both the sender and the recipient.
Liquidity Management: RTGS systems help banks manage liquidity by providing real-time visibility into their cash positions and facilitating efficient fund transfers.
Support for Financial Markets: RTGS systems play a crucial role in supporting financial markets by enabling timely settlement of securities transactions and interbank transfers.

2.3.5 Costs:

- RTGS transactions often incur higher fees compared to other payment modes due to the immediate and guaranteed settlement provided.
- The cost structure may vary depending on factors such as the transaction amount, the jurisdiction, and the policies of the participating banks or central bank.

2.3.6 Regulation and Oversight:

- RTGS systems are subject to regulation and oversight by central banks or monetary authorities to ensure safety, efficiency, and stability in the financial system.
- Regulatory requirements may include adherence to security standards, operational resilience, and compliance with anti-money laundering (AML) and know-your-customer (KYC) regulations.

2.3.7 Future Trends:

Integration with Instant Payment Systems: RTGS systems may evolve to integrate with instant payment systems, providing seamless connectivity between high-value and retail payment channels.
Enhanced Efficiency: Continuous improvements in technology and infrastructure may lead to enhanced efficiency and scalability of RTGS systems, reducing processing times and operational costs.
Global Interoperability: Efforts to enhance interoperability between RTGS systems across different jurisdictions may facilitate cross-border transactions and promote international trade and investment.

2.4 National Electronic Funds Transfer (NEFT)

National Electronic Funds Transfer (NEFT) is a widely used electronic payment mode in India, offering convenience, affordability, and widespread coverage for transferring funds between bank accounts. While NEFT transactions are processed in batches with deferred settlement, ongoing efforts to enhance processing speed and operational efficiency are expected to further improve the user experience and accessibility of the service.

Definition: NEFT is an electronic payment system operated by the Reserve Bank of India (RBI) that facilitates interbank transfers of funds on a deferred net settlement (DNS) basis. It allows individuals, businesses, and institutions to transfer funds electronically from one bank account to another.

2.4.1 Key Features:

Deferred Settlement: NEFT transactions are processed in batches at set intervals throughout the day, rather than in real-time. Settlement occurs on a net basis, where transactions are grouped and settled periodically.

Availability: NEFT transactions can be initiated and processed on all working days of banks in India, including Saturdays, except for Sundays and designated holidays.

No Minimum or Maximum Transaction Limit: NEFT does not have a minimum or maximum transaction limit, allowing for the transfer of both small and large sums of money.

Widely Used: NEFT is widely adopted by individuals, businesses, and institutions for various purposes, including salary payments, bill payments, online purchases, and remittances.

2.4.2 Process:

Initiation: The sender initiates a NEFT transaction through their bank, providing details such as the recipient's account number, the name of the beneficiary bank, the branch IFSC (Indian Financial System Code) code, and the amount to be transferred.

Processing: The sender's bank aggregates all NEFT transactions received up to a specified cutoff time and forwards them to the RBI's NEFT system for processing.

Settlement: The NEFT system processes transactions in batches and settles them at predetermined intervals, typically hourly during business hours.

Credit to Beneficiary: Once the transaction is settled, the funds are credited to the recipient's bank account. The recipient's bank then notifies the recipient of the credit.

2.4.3 Operating Hours:

- NEFT transactions can be initiated and processed during the working hours of banks in India, including Saturdays, except for Sundays and designated holidays.
- Banks may have specific cutoff times for accepting NEFT transactions, beyond which transactions are queued for processing in the next available batch.

2.4.4 Benefits:

Convenience: NEFT provides a convenient and accessible way to transfer funds electronically between bank accounts, eliminating the need for physical cash or checks.

Cost-Effective: NEFT transactions typically incur lower fees compared to other electronic payment modes, making it an affordable option for individuals and businesses.

Widespread Coverage: NEFT is supported by a vast network of banks across India, ensuring widespread coverage and accessibility for users.

Secure: NEFT transactions are processed through secure channels and adhere to strict regulatory guidelines, ensuring the safety and integrity of funds transferred.

2.4.5 Challenges:

Processing Delays: Since NEFT transactions are processed in batches at set intervals, there may be delays in fund transfers, especially for transactions initiated close to cutoff times.

Limited Operating Hours: NEFT transactions can only be initiated during the working hours of banks, which may restrict the availability of the service for users.

Transaction Limits: While NEFT does not have a maximum transaction limit, individual banks may impose daily or per-transaction limits on NEFT transfers for security and compliance purposes.

2.4.6 Future Trends:

Enhanced Processing Speed: Efforts to improve the efficiency and speed of NEFT transactions may lead to shorter processing times and faster fund transfers.

Extended Operating Hours: Some banks may extend their operating hours for NEFT transactions to provide greater flexibility and convenience for users.

Integration with Instant Payment Systems: Integration with instant payment systems like Unified Payments Interface (UPI) may enable faster and more seamless fund transfers between NEFT and UPI accounts.

2.5 Summary

In this lesson, we delve into the realm of electronic data interchange (EDI) alongside two prominent electronic payment modes: National Electronic Funds Transfer (NEFT) and Real-Time Gross Settlement (RTGS). We begin by exploring the fundamentals of EDI, elucidating its role in facilitating standardized and automated exchange of business documents. Transitioning to NEFT, we dissect the operational processes, benefits, and limitations of this widely utilized electronic fund transfer mechanism within India's banking system. Next, we unravel the intricacies of RTGS, dissecting its real-time settlement capabilities and suitability for high-value transactions. Through comparative analysis, learners gain a nuanced understanding of the distinct features and applications of each mode, enabling them to navigate the complexities of modern electronic transactions with confidence.

2.6 Keywords

Blockchain Integration: Blockchain technology has the potential to enhance the security and traceability of EDI transactions by providing a tamper-resistant and transparent ledger of transactions.

Digital Wallets: Digital wallets store payment information securely and can be used to make payments in-store, online, or via mobile devices. Examples include PayPal, Venmo, and Cash App.

Biometric Authentication: Biometric technologies like fingerprint scanning and facial recognition are increasingly being used to enhance security and streamline authentication for electronic payments.

Embedded Payments: Payments integrated into Internet of Things (IoT) devices, smart appliances, and wearable devices enable seamless transactions as part of everyday activities.**Liquidity Management:** RTGS systems help banks manage liquidity by providing real-time visibility into their cash positions and facilitating efficient fund transfers.

2.7 Self-Assessment Questions

1. What is the primary purpose of Electronic Data Interchange (EDI), and how does it streamline business processes?
2. Describe the key differences between National Electronic Funds Transfer (NEFT) and Real-Time Gross Settlement (RTGS) payment modes, including their transaction processing times and settlement mechanisms.

3. How does NEFT facilitate fund transfers between bank accounts within India, and what are its operating hours and transaction limits?
4. What are the benefits and limitations of using RTGS for high-value transactions, and what factors should be considered when choosing between NEFT and RTGS?
5. Discuss the role of electronic payment modes in enhancing efficiency, security, and transparency in financial transactions, citing examples from real-world applications.
6. Explain the concept of batch processing in electronic payment systems and its implications for transaction processing times in NEFT and RTGS.
7. How do regulatory requirements and industry standards influence the design, implementation, and operation of electronic data interchange and electronic payment modes, and what measures are taken to ensure compliance and security?

2.8 Suggested Readings

1. William H. Sprague, Jr (1990). Electronic Data Interchange: Concepts and Applications. Prentice Hall.
2. Hooman Estelami (2010). Electronic Payment Systems: A User-Centered Perspective and Interaction Design. Cambridge University Press.
3. Rajeev Bhandari (2015). National Electronic Funds Transfer (NEFT): A Comprehensive Guide. McGraw-Hill Education
4. Agustin Carstens and Liliana Rojas-Suarez (2007). Real-Time Gross Settlement Systems: An Overview. International Monetary Fund
5. Donald O'Mahony and Tim Peirce (2001). Electronic Payment Systems: Technology and Implementation. Artech House
6. David Bannister and Nicolas Huss (2019). Digital Payments and the Emerging Payments Landscape. Palgrave Macmillan
7. Carol Coye Benson and Scott Loftesness (2015). Payments Systems in the U.S. - Second Edition: A Guide for the Payments Professional. Glenbrook Partners.

Dr. Nagaraju Battu

Lesson- 3
EXPLORING VIRTUAL CURRENCIES: BITCOIN AND SECURITY CONSIDERATIONS

Learning objectives

- To Define Bitcoin and virtual currencies, explaining their fundamental characteristics
- To Explore the underlying technology of Bitcoin, including blockchain, decentralized ledgers, and cryptographic techniques.
- To Discuss the role of mining in the Bitcoin network
- To Investigate the potential vulnerabilities and risks within the Bitcoin ecosystem

Structure

3.0 Introduction

Virtual currencies, often referred to as cryptocurrencies, have emerged as revolutionary digital assets in the realm of finance and technology. These decentralized digital currencies utilize cryptographic techniques to secure transactions and regulate the creation of new units. Offering borderless, instant, and relatively anonymous transactions, virtual currencies have transformed the way we perceive and engage in financial transactions, challenging traditional banking systems and fostering innovations in various sectors worldwide.

3.1 E-Cash

E-cash, short for electronic cash, refers to digital currency that is stored, transmitted, and used electronically. It is a form of currency that exists only in electronic form and facilitates online transactions without the need for physical cash or traditional banking systems.

While e-cash offers convenience and efficiency, it also presents various security concerns that users and businesses must consider. These concerns primarily revolve around security, anonymity, and traceability.

3.1.1 Security Issues with E-Cash

Fraud and Identity Theft:

One of the primary security concerns with e-cash is the risk of fraud and identity theft. Hackers and cybercriminals may exploit vulnerabilities in e-cash systems to steal funds or sensitive personal information, leading to financial losses and privacy breaches.

Phishing and Social Engineering Attacks:

Phishing attacks, where attackers impersonate legitimate entities to trick users into revealing their credentials or financial information, are common in e-cash systems. Social engineering techniques are also used to manipulate users into divulging sensitive information.

Cybersecurity Threats:
E-cash systems are susceptible to various cybersecurity threats, including malware, ransomware, and distributed denial-of-service (DDoS) attacks. These threats can disrupt e-cash services, compromise user accounts, and cause financial harm to individuals and businesses.

3.1.2 Anonymity in E-Cash Transactions

Anonymity vs. Pseudonymity:
E-cash transactions offer varying degrees of anonymity, depending on the design of the system. Some e-cash systems provide full anonymity, while others offer pseudonymity, where transactions are recorded using cryptographic addresses instead of real-world identities.

Privacy Concerns:
While anonymity can protect user privacy and prevent unauthorized surveillance, it also raises concerns about illegal activities, such as money laundering, tax evasion, and illicit transactions on the dark web. Regulators and law enforcement agencies often seek to balance privacy with security and regulatory compliance.

3.1.3 Traceability and Transparency

Transaction Traceability:
Despite the anonymity or pseudonymity provided by some e-cash systems, transactions are often traceable on the blockchain or transaction ledger. Blockchain analysis tools allow investigators to trace the flow of funds and identify patterns of activity, aiding in law enforcement efforts and regulatory compliance.

Regulatory Compliance:
E-cash systems must adhere to regulatory requirements, such as anti-money laundering (AML) and know-your-customer (KYC) regulations, to prevent illicit activities and ensure financial transparency. Compliance with these regulations may involve implementing identity verification measures and transaction monitoring systems.

3.1.4 Mitigating E-Cash Security Risks

Encryption and Secure Protocols:
E-cash systems should employ robust encryption techniques and secure communication protocols to protect sensitive information and prevent unauthorized access. This includes implementing strong cryptographic algorithms and using secure channels for data transmission.

Multi-factor Authentication:
Implementing multi-factor authentication (MFA) can enhance e-cash security by requiring users to provide multiple forms of verification, such as passwords, biometrics, or one-time codes. MFA adds an extra layer of protection against unauthorized access and identity theft.

Education and Awareness:
Educating users about e-cash security risks and best practices is essential for promoting safe usage. Training programs, awareness campaigns, and informational resources can help users

recognize potential threats, avoid common pitfalls, and take proactive steps to protect their e-cash assets.

E-cash offers numerous benefits, but it also poses security challenges related to fraud, anonymity, and traceability. By addressing these concerns through robust security measures, regulatory compliance, and user education, e-cash systems can provide a secure and trustworthy platform for electronic transactions.

3.2 Virtual Currencies

Virtual currencies, also known as cryptocurrencies, are digital or virtual representations of value that operate as a medium of exchange. Unlike traditional currencies issued by governments (fiat currencies), virtual currencies rely on cryptographic techniques to secure transactions and control the creation of new units. The first and most well-known virtual currency is Bitcoin, introduced in 2009 by an unknown person or group using the pseudonym Satoshi Nakamoto.

3.2.1 Key Characteristics:

1. Decentralization: Virtual currencies typically operate on decentralized networks, such as blockchain, which eliminates the need for a central authority like a bank or government.
2. Anonymity: Transactions made with virtual currencies often provide a level of anonymity, as users are identified by cryptographic addresses rather than personal information.
3. Limited Supply: Many virtual currencies have a finite supply, meaning there is a maximum number of units that can ever exist. For example, Bitcoin has a maximum supply of 21 million coins.
4. Global Accessibility: Virtual currencies can be accessed and used by anyone with an internet connection, enabling borderless transactions.

3.2.2 Sub-systems of Virtual Currencies

Blockchain Technology:

Virtual currencies like Bitcoin rely on blockchain technology to record transactions securely and immutably. A blockchain is a decentralized ledger that stores all transaction data across a network of computers. Each transaction is verified by network participants (miners) through cryptographic algorithms and added to a block, which is then appended to the existing chain of blocks, hence the term "blockchain."

Mining:

Mining is the process by which new virtual currency units are created and transactions are verified. Miners use powerful computers to solve complex mathematical problems, and in return, they are rewarded with newly created virtual currency units. This process also helps secure the network and validate transactions.

Wallets:

Virtual currency wallets are digital tools used to store, send, and receive virtual currencies. Wallets come in various forms, including software wallets (applications), hardware wallets (physical devices), and paper wallets (printed QR codes).

Transaction Process:

When a user initiates a transaction using virtual currency, the transaction is broadcasted to the network and included in a block for verification. Once verified, the transaction is added to the blockchain and becomes irreversible.

3.2.3 Virtual Currencies Life Cycle

The cycle of virtual currencies can be understood through various stages, each reflecting different aspects of their development, adoption, and eventual fate. The cycle of virtual currencies is dynamic and nonlinear. Different currencies may progress through these stages at varying paces, and the outcomes can be influenced by a wide range of factors, including technology advancements, regulatory developments, market dynamics, and community support.Here is a breakdown of the typical virtual currency cycle:

1. Inception and Innovation: Virtual currencies are born out of innovative ideas, often aiming to address specific shortcomings in traditional financial systems or to pioneer new use cases enabled by blockchain technology. This stage involves the conceptualization of the currency, development of its underlying technology, and the creation of a community around the project.

2. Initial Coin Offering (ICO) or Token Sale: To fund development and kickstart adoption, virtual currencies often undergo an ICO or token sale. During this stage, the project's tokens are offered to investors and early adopters in exchange for other cryptocurrencies or fiat currency. This provides the initial capital needed to fund development and operations.

3. Speculative Frenzy and Volatility: Following the ICO, the virtual currency typically experiences a period of intense speculation and price volatility. Investors and traders buy and sell the currency on exchanges, often driven by hype, speculation, and market sentiment. Prices can experience rapid fluctuations during this phase, influenced by factors such as news, market trends, and investor sentiment.

4. Adoption and Integration: As the virtual currency gains traction, developers, businesses, and individuals start integrating it into their systems and processes. This stage is marked by increasing adoption and usage across various sectors, including finance, gaming, supply chain management, and more. Merchant acceptance grows, and the currency starts to fulfill its intended use cases.

5. Regulatory Scrutiny and Compliance: With increasing adoption comes regulatory scrutiny. Governments and regulatory bodies begin to formulate policies and regulations to govern the use of virtual currencies, exchanges, and related activities. Compliance with these regulations becomes crucial for the continued operation and legitimacy of the currency.

6. Market Maturation or Consolidation: Virtual currencies that successfully navigate regulatory challenges and gain widespread adoption enter a phase of market maturation. This stage is characterized by a more stable market environment, with established players and infrastructure. Some currencies may undergo consolidation through mergers, acquisitions, or partnerships to strengthen their position in the market.

7. Mainstream Acceptance or Obsolescence: Virtual currencies that achieve mainstream acceptance become integrated into everyday life and financial systems. They serve as viable alternatives to traditional currencies and payment methods, offering benefits such as faster transactions, lower fees, and increased accessibility. However, currencies that fail to gain sufficient adoption or overcome regulatory hurdles may become obsolete and fade into obscurity.

8. Continuous Evolution and Innovation: Even after achieving mainstream acceptance, virtual currencies continue to evolve and innovate. Developers work on improving scalability, security, and functionality to address new challenges and opportunities. New use cases and applications for blockchain technology emerge, driving further innovation in the space.

3.2.4 Advantages and Disadvantages of Virtual Currencies

Advantages:

Decentralization: Virtual currencies operate without the need for a central authority, providing users with more control over their finances.

Lower Transaction Fees: Transactions with virtual currencies often incur lower fees compared to traditional banking systems, especially for international transfers.

Global Accessibility: Virtual currencies enable individuals to participate in the global economy, regardless of their geographic location or banking infrastructure.

Security: Blockchain technology ensures the security and immutability of transactions, reducing the risk of fraud and unauthorized activity.

Disadvantages:

1. Volatility: Virtual currencies are known for their price volatility, with values fluctuating significantly over short periods.

2. Regulatory Uncertainty: The regulatory environment surrounding virtual currencies varies by country and is subject to change, creating uncertainty for users and investors.

3. Risk of Theft: While blockchain technology is secure, virtual currency holdings are still vulnerable to hacking and theft, especially if proper security measures are not implemented.

4. Limited Acceptance: Despite growing acceptance, virtual currencies are not universally accepted as a form of payment, limiting their usability in some contexts.

3.2.5 Real-world Applications of Virtual Currencies

Remittances:

Virtual currencies are increasingly used for cross-border remittance payments, allowing individuals to send money to family members or friends in other countries with lower fees and faster transaction times compared to traditional remittance services.

Online Retail:

Several online retailers and service providers accept virtual currencies as payment, offering consumers an alternative to traditional payment methods. For example, Overstock.com and Shopify allow customers to pay with Bitcoin and other virtual currencies.

Investment:

Virtual currencies have emerged as a new asset class for investors, with many individuals and institutions buying and holding virtual currencies as a long-term investment. Some investors also engage in trading virtual currencies on exchanges to profit from price fluctuations.

Decentralized Finance (DeFi):

Decentralized finance refers to financial services and applications built on blockchain technology, including lending, borrowing, and trading, without the need for traditional intermediaries like banks. Virtual currencies play a central role in many DeFi platforms, enabling users to access financial services in a permissionless and transparent manner.

Examples:
- Bitcoin (BTC)
- Ethereum (ETH)
- Ripple (XRP)
- Litecoin (LTC)
- Bitcoin Cash (BCH)

3.3 Bitcoin (BTC)

Definition: Bitcoin, abbreviated as BTC, is a decentralized digital currency that operates on a peer-to-peer network without the need for intermediaries such as banks or governments.

Genesis: Bitcoin was conceptualized in a 2008 whitepaper titled "Bitcoin: A Peer-to-Peer Electronic Cash System" by an individual or group using the pseudonym Satoshi Nakamoto. It was released as open-source software in January 2009.

3.3.1 How Bitcoin Works:

1. Blockchain Technology:

- Bitcoin operates on a blockchain, which is a distributed ledger that records all transactions across a network of computers.
- Blocks containing multiple transactions are added to the blockchain in a sequential and immutable manner.
- Each block is cryptographically linked to the previous one, forming a chain of blocks, hence the term "blockchain."

2. Decentralization:

- Bitcoin operates without a central authority, making it resistant to censorship and control by any single entity.
- Transactions are verified and recorded by network participants called miners, who use computational power to solve complex mathematical puzzles.

3. Cryptographic Security:

- Transactions on the Bitcoin network are secured using cryptographic algorithms.
- Private keys are used to sign transactions, ensuring that only the owner of the bitcoins can spend them.
- Public keys, derived from private keys, are used to generate unique addresses where bitcoins can be sent and received.

3.3.2 Key Characteristics of Bitcoin:

1. Limited Supply:

- The total supply of Bitcoin is capped at 21 million coins, a rule hardcoded into the protocol.
- This scarcity is enforced through a process called the "halving," which reduces the rate of new bitcoin issuance approximately every four years until the maximum supply is reached.

2. Volatility:

- Bitcoin's price has exhibited significant volatility since its inception, with prices experiencing rapid fluctuations over short periods of time.

- Factors influencing Bitcoin's price include market demand, investor sentiment, regulatory developments, and macroeconomic trends.

3. Anonymity and Pseudonymity:

- While Bitcoin transactions are recorded on the blockchain, the identities of the parties involved are not directly linked to their public addresses.
- This provides a certain degree of privacy and pseudonymity, although transactions can be traced and analyzed using blockchain analysis tools.

3.3.3 Uses and Applications of Bitcoin:

1. Store of Value:

- Many proponents consider Bitcoin to be a digital alternative to gold, serving as a store of value and a hedge against inflation.
- Its limited supply and decentralized nature make it attractive for long-term investors seeking to preserve wealth.

2. Medium of Exchange:

- Bitcoin can be used as a medium of exchange for goods and services, although its adoption for everyday transactions remains limited.
- Some merchants and businesses accept Bitcoin payments, and the development of payment solutions and merchant services continues to facilitate its use in commerce.

3. Investment and Speculation:

- Bitcoin has gained significant attention from investors, traders, and speculators seeking to profit from its price movements.
- Investment vehicles such as Bitcoin exchange-traded funds (ETFs), futures contracts, and investment trusts provide avenues for exposure to Bitcoin's price without directly holding the underlying asset.

3.3.4 Risks and Challenges:

1. Price Volatility:

- Bitcoin's price volatility exposes investors to significant risks, with the potential for substantial gains or losses over short periods of time.
- Price fluctuations can be influenced by market sentiment, regulatory developments, technological advancements, and macroeconomic factors.

2. Regulatory Uncertainty:

- Regulatory developments and government interventions can impact the adoption and use of Bitcoin.
- Regulatory frameworks vary by jurisdiction, with some countries embracing Bitcoin and others imposing restrictions or outright bans on its use.

3. Security Concerns:

- While Bitcoin's blockchain is considered secure, individual users may be vulnerable to hacks, scams, and theft if they fail to adequately protect their private keys and wallets.
- Risks include phishing attacks, malware, exchange hacks, and social engineering exploits.

3.4 Other Virtual Currencies

Ethereum (ETH):

Function: Ethereum is a decentralized platform that enables the creation and execution of smart contracts and decentralized applications (DApps). It serves as a programmable blockchain, allowing developers to build a wide range of decentralized applications.

Differences: Ethereum introduces the concept of smart contracts, self-executing contracts with the terms of the agreement directly written into code. It operates on a proof-of-stake consensus mechanism and has no fixed supply, with new coins created through staking rewards.

Example: A decentralized finance (DeFi) platform is built on the Ethereum blockchain, allowing users to borrow, lend, and trade assets without the need for traditional financial intermediaries, providing greater accessibility and transparency.

Ripple (XRP):

Function: Ripple is a digital payment protocol and cryptocurrency designed for fast, low-cost cross-border transactions. It aims to facilitate real-time settlement of payments between financial institutions and other entities.

Differences: Ripple operates on a consensus algorithm known as the Ripple Protocol Consensus Algorithm (RPCA), which does not require mining like Bitcoin. It is primarily used by banks and financial institutions for international remittances and liquidity management.

Example: A multinational bank adopts Ripple's technology to streamline its cross-border payment processes, reducing transaction costs and settlement times for its customers while improving overall efficiency.

Litecoin (LTC):

Function: Litecoin is a peer-to-peer cryptocurrency that aims to complement Bitcoin by offering faster transaction times and lower fees. It serves as a digital alternative to fiat currencies for everyday transactions.

Differences: Litecoin uses a different hashing algorithm (Scrypt) than Bitcoin, resulting in faster block generation times and a larger maximum supply of 84 million coins. It is often considered the "silver" to Bitcoin's "gold."

Example: A retail merchant begins accepting Litecoin as a payment method alongside traditional fiat currencies, attracting tech-savvy customers who value the faster transaction speeds and lower fees offered by Litecoin.

Bitcoin Cash (BCH):

Function: Bitcoin Cash is a cryptocurrency that emerged as a result of a hard fork from Bitcoin in 2017. It aims to improve upon Bitcoin's scalability and transaction speed by increasing the block size limit.

Differences: Bitcoin Cash increases the block size limit to 8 MB compared to Bitcoin's 1 MB, allowing for more transactions to be processed per block. It also aims to lower transaction fees and improve usability as a medium of exchange.

Example: An online retailer integrates Bitcoin Cash as a payment option on its website, attracting customers who prefer using cryptocurrencies for online purchases due to lower fees and faster transaction confirmations.

3.5 Future Trends and Challenges

Future Trends:

1. Mainstream Adoption: Virtual currencies are expected to continue moving towards mainstream adoption, with more businesses and consumers embracing their use for everyday transactions.

2. Interoperability: Efforts to improve interoperability between different virtual currencies and blockchain networks could facilitate greater efficiency and connectivity within the virtual currency ecosystem.

3. Regulatory Clarity: Clearer regulatory frameworks and guidelines are likely to emerge, providing greater certainty for users, investors, and businesses operating in the virtual currency space.

4. Technological Innovations: Ongoing technological advancements, such as the development of scalable blockchain solutions and improvements in security and privacy features, are expected to further enhance the capabilities of virtual currencies.

Challenges:

1. Scalability: Scaling issues, such as slow transaction processing times and high fees during periods of network congestion, remain significant challenges for widespread adoption of virtual currencies.

2. Regulatory Hurdles: Regulatory uncertainty and differing approaches to virtual currency regulation across jurisdictions could hinder growth and innovation in the virtual currency space.

3. Security Concerns: As virtual currency usage grows, so too do security threats, including hacking, fraud, and scams. Addressing these security concerns is crucial to maintaining user trust and confidence in virtual currencies.

4. Environmental Impact: The energy consumption associated with virtual currency mining, particularly for proof-of-work-based cryptocurrencies like Bitcoin, has raised concerns about the environmental sustainability of virtual currency networks.

3.6 Summary

In this comprehensive lesson on "Exploring Virtual Currencies: Bitcoin and Security Considerations," we delve into the intricate world of Bitcoin and its underlying security dynamics. Beginning with an elucidation of Bitcoin's core principles and its departure from conventional currency systems, we navigate through the intricacies of blockchain technology, decentralized ledgers, and cryptographic protocols that underpin its operation. We meticulously dissect the multifaceted security landscape of Bitcoin, scrutinizing issues such as private key management, wallet security, and the role of miners in upholding network integrity. Moreover, we delve into potential vulnerabilities like 51% attacks and double spending, coupled with the regulatory challenges that surround Bitcoin's decentralized nature. Through real-world case studies and proactive strategies for mitigating security risks, learners gain a profound understanding of the critical nexus between security considerations and the widespread adoption of virtual currencies like Bitcoin, enabling them to navigate this evolving landscape with confidence and diligence.

3.7 Keywords

Cybersecurity Threats:E-cash systems are susceptible to various cybersecurity threats, including malware, ransomware, and distributed denial-of-service (DDoS) attacks. These threats can disrupt e-cash services, compromise user accounts, and cause financial harm to individuals and businesses.

Transaction Traceability: Despite the anonymity or pseudonymity provided by some e-cash systems, transactions are often traceable on the blockchain or transaction ledger. Blockchain analysis tools allow investigators to trace the flow of funds and identify patterns of activity, aiding in law enforcement efforts and regulatory compliance.

Mining: Mining is the process by which new virtual currency units are created and transactions are verified. Miners use powerful computers to solve complex mathematical problems, and in return, they are rewarded with newly created virtual currency units. This process also helps secure the network and validate transactions.

Wallets: Virtual currency wallets are digital tools used to store, send, and receive virtual currencies. Wallets come in various forms, including software wallets (applications), hardware wallets (physical devices), and paper wallets (printed QR codes).

Remittances: Virtual currencies are increasingly used for cross-border remittance payments, allowing individuals to send money to family members or friends in other countries with lower fees and faster transaction times compared to traditional remittance services.

3.8 Self-Assessment Questions

1. What are the fundamental characteristics that distinguish Bitcoin from traditional forms of currency?
2. Explain the role of blockchain technology in ensuring the security and integrity of the Bitcoin network.
3. Discuss the importance of private key management in securing Bitcoin transactions and wallets.
4. What are the potential risks and vulnerabilities associated with Bitcoin, such as 51% attacks and double spending?
5. How do miners contribute to the security of the Bitcoin network, and what incentives do they have for maintaining network integrity?
6. Analyze the impact of regulatory challenges on the security and adoption of Bitcoin as a virtual currency.
7. Evaluate strategies and best practices for securing Bitcoin assets and mitigating security risks for individual users and businesses.
8. Provide examples of real-world case studies involving security breaches or incidents related to Bitcoin, and discuss lessons learned.
9. How do security considerations influence public perception, adoption rates, and the overall stability of virtual currencies like Bitcoin?
10. Reflect on the interplay between security considerations and the evolution of Bitcoin and other virtual currencies, considering future trends and challenges.

3.9 Suggested Readings

1. Andreas M. Antonopoulos (2014). Mastering Bitcoin: Unlocking Digital Cryptocurrencies. O'Reilly Media
2. Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder (2016). Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press
3. Antony Lewis (2018). The Basics of Bitcoins and Blockchains: An Introduction to Cryptocurrencies and the Technology that Powers Them. Lioncrest Publishing).
4. Chris Burniske and Jack Tatar (2017). Cryptoassets: The Innovative Investor's Guide to Bitcoin and Beyond. McGraw-Hill Education
5. Daniel Drescher (2017). Blockchain Basics: A Non-Technical Introduction in 25 Steps. Apress.

Dr. B. Sreedhar Reddy

Lesson- 4
UNDERSTANDING AUTOMATED CLEARING AND SETTLEMENTS

Learning Objectives

- To Define Automated Clearing and Settlements (ACS)
- To Explore the technological foundations and infrastructure of ACS systems
- To Analyze the benefits and challenges associated with ACS
- To Evaluate the risk management practices governing ACS

Structure

4.0 Introduction to Clearing and Settlement

Definition: Clearing and settlement are essential processes in financial markets that ensure the efficient and timely completion of transactions. Clearing involves matching and validating trades, while settlement involves the transfer of funds and securities between parties.

Traditional vs. Automated Clearing and Settlement:

Traditionally, clearing and settlement processes were manual and paper-based, leading to delays, errors, and higher costs.

Automated clearing and settlement (ACS) systems leverage technology to streamline and automate these processes, reducing risk, enhancing efficiency, and increasing transparency.

4.1 A Brief History of Automated Clearing and Settlement Systems

Automated Clearing and Settlement Systems (ACSS) have played a pivotal role in the modernization and efficiency of financial markets worldwide. Understanding the evolution of these systems is essential for grasping their significance in facilitating secure and timely transactions. The history of ACSS dates back to the mid-20th century, characterized by a gradual transition from manual to automated processes, driven by technological advancements and the need for increased efficiency in financial operations.

In the early stages of financial markets, clearing and settlement processes were predominantly manual, relying heavily on paper-based documentation and human intervention. This manual system was labour-intensive, prone to errors, and lacked the speed required to keep pace with the growing volume of transactions. Consequently, financial institutions sought innovative solutions to streamline these processes and reduce operational risks.

The emergence of computers and telecommunications technology in the latter half of the 20th century revolutionized the landscape of financial services. This technological revolution laid the groundwork for the automation of clearing and settlement systems. In the 1960s and 1970s, financial institutions began experimenting with computerized systems to handle payment processing more efficiently. These early systems were rudimentary compared to modern standards but represented a significant step towards automation.

One of the milestone developments in the history of ACSS was the introduction of electronic funds transfer (EFT) systems in the 1970s. EFT systems allowed for the electronic exchange of funds between financial institutions, eliminating the need for physical movement of checks or cash. This innovation significantly accelerated transaction processing times and reduced the reliance on paper-based instruments.

The 1980s witnessed further advancements in ACSS with the introduction of real-time gross settlement (RTGS) systems. Unlike traditional batch processing systems, RTGS systems enable transactions to be settled individually and immediately upon submission. This real-time settlement mechanism minimizes credit and liquidity risks, enhancing the stability and efficiency of financial markets.

The globalization of financial markets in the late 20th and early 21st centuries further fueled the evolution of ACSS. Cross-border transactions necessitated interoperability between different clearing and settlement systems, leading to the development of international standards and frameworks. Initiatives such as the Continuous Linked Settlement (CLS) system emerged to mitigate foreign exchange settlement risk and foster greater efficiency in global payment processing.

In recent years, technological innovations such as blockchain technology and distributed ledger systems have presented new possibilities for ACSS. These decentralized technologies offer the potential to streamline clearing and settlement processes, enhance transparency, and reduce counterparty risks. However, widespread adoption of these technologies in mainstream financial markets remains a subject of ongoing exploration and debate.

The history of Automated Clearing and Settlement Systems reflects a journey of continuous innovation and adaptation to meet the evolving needs of financial markets. From manual paper-based processes to sophisticated electronic systems, the evolution of ACSS has been driven by technological progress, regulatory changes, and the quest for efficiency and risk mitigation. Looking ahead, the ongoing digitization and globalization of financial services are likely to shape the future trajectory of ACSS, paving the way for more efficient, secure, and interconnected payment systems.

4.2 Automated Clearing and Settlement Systems in India

The evolution of Automated Clearing and Settlement (ACS) systems in India reflects the country's journey towards modernization and digitization of its financial infrastructure. The early stages of ACS systems in India can be traced back to the introduction of electronic payment mechanisms in the 1980s and 1990s. During this period, initiatives such as Electronic Funds Transfer (EFT) and Electronic Clearing Service (ECS) were launched to facilitate electronic fund transfers and recurring payments, laying the foundation for future developments in ACS systems.

The turning point in the history of ACS systems in India came with the establishment of the National Electronic Funds Transfer (NEFT) system in November 2005 by the Reserve Bank of India (RBI). NEFT revolutionized the way funds were transferred between banks by enabling electronic transfer of funds on a nationwide basis. NEFT operates on a deferred net settlement (DNS) basis, where transactions are batched and settled in hourly batches throughout the day, providing a cost-effective and efficient means of fund transfer for businesses and individuals across India.

Following the success of NEFT, the Reserve Bank of India introduced the Real Time Gross Settlement (RTGS) system in March 2004 to facilitate real-time electronic funds transfer and settlement of high-value transactions. RTGS operates on a gross basis, where transactions are settled individually and in real-time, providing immediate finality of funds transfer. The introduction of RTGS marked a significant milestone in the history of ACS systems in India, enabling faster and more secure settlement of high-value transactions in the country's financial markets.

In addition to NEFT and RTGS, the Securities and Exchange Board of India (SEBI) introduced the Securities Settlement System (SSS) in 1998 to facilitate electronic settlement of securities trades in Indian stock exchanges. The SSS enables seamless transfer of securities between buyers and sellers, reducing settlement risk and enhancing efficiency in the Indian capital markets. Over the years, the SSS has undergone various enhancements and upgrades to meet the evolving needs of market participants and regulatory requirements.

Furthermore, the introduction of the Unified Payments Interface (UPI) in 2016 marked a significant milestone in the evolution of ACS systems in India. UPI is a real-time payment system developed by the National Payments Corporation of India (NPCI) that enables instant fund transfers between bank accounts using a mobile phone. UPI has gained widespread adoption in India due to its convenience, speed, and interoperability across banks and payment service providers, further advancing the digitization of payment systems in the country.

The history of Automated Clearing and Settlement Systems in India reflects the country's commitment to embracing technological innovation and modernizing its financial infrastructure. From the early initiatives such as EFT and ECS to the introduction of NEFT, RTGS, SSS, and UPI, India has witnessed a remarkable transformation in its payment and settlement systems over the years. These developments have not only improved efficiency, transparency, and security in the financial markets but have also facilitated greater financial inclusion and economic growth across the country.

4.3 Components of Automated Clearing and Settlement Systems

1. Clearinghouse:

- A clearinghouse acts as an intermediary between buyers and sellers, facilitating the clearing and settlement of transactions.
- It verifies the authenticity of trades, nets positions, calculates obligations, and ensures that transactions are completed in compliance with regulatory requirements.

2. Central Securities Depository (CSD):

- A CSD is a specialized financial institution responsible for the safekeeping and administration of securities.
- It facilitates the transfer of ownership and provides services such as custody, settlement, and asset servicing.

3. Payment Systems:

- Payment systems enable the transfer of funds between participants in a transaction.
- They support various payment instruments, including wire transfers, automated clearinghouse (ACH) transactions, and real-time gross settlement (RTGS) systems.

4.4 Key Features of Automated Clearing and Settlement Systems

1. Real-time Processing:

- ACS systems enable real-time processing of transactions, allowing for instantaneous validation, clearing, and settlement.
- Real-time processing reduces counterparty risk and enhances liquidity by accelerating the availability of funds and securities.

2. Straight-Through Processing (STP):

- STP automates the end-to-end processing of transactions without manual intervention.
- It eliminates the need for rekeying data, reducing errors, and speeding up the settlement process.

3. Netting:

- Netting involves offsetting transactions to reduce the overall amount of funds or securities that need to be exchanged.
- Netting optimizes liquidity, reduces settlement risk, and minimizes the number of transactions processed.

4.5 Objectives of Automated Clearing and Settlement Systems

Automated Clearing and Settlement (ACS) systems are designed with several overarching objectives aimed at enhancing the efficiency, reducing risks, and improving the overall functioning of financial markets. One of the primary objectives of ACS systems is to streamline the clearing and settlement processes. Historically, these processes were manual, time-consuming, and prone to errors. By automating key tasks such as trade matching, validation, and settlement, ACS systems significantly reduce the time required to complete transactions. Real-time processing capabilities enable swift validation and settlement, minimizing delays and ensuring timely execution of trades. This efficiency not only saves time but also reduces operational costs for market participants, including financial institutions, brokers, and investors.

Another key objective of ACS systems is risk mitigation. Manual clearing and settlement processes were vulnerable to various risks, including operational errors, fraud, and settlement failures. By automating these processes and implementing robust risk management measures, ACS systems help minimize counterparty risk, settlement risk, and operational risk. Real-time monitoring and surveillance tools enable early detection of anomalies or irregularities, allowing for prompt intervention and risk mitigation strategies. Additionally, the transparency provided by ACS systems enhances market integrity and confidence, reducing the potential for market abuse and misconduct.

Efficiency and risk mitigation aside, ACS systems also aim to improve liquidity and optimize capital efficiency in financial markets. Traditional settlement methods often required participants to hold excess liquidity to cover settlement obligations, tying up capital that could otherwise be deployed more productively. ACS systems leverage netting and optimization techniques to minimize the overall amount of funds or securities that need to be exchanged, thereby reducing liquidity requirements and freeing up capital for other purposes. Real-time settlement capabilities enhance liquidity by accelerating the availability of funds and securities, enabling participants to deploy capital more efficiently and seize investment opportunities without delay.

Furthermore, ACS systems contribute to enhancing transparency, compliance, and regulatory oversight in financial markets. Manual processes lacked the transparency and audit trails necessary to track and monitor transactions effectively, making it challenging to enforce regulatory requirements and detect potential instances of market abuse or misconduct. ACS systems provide real-time visibility into transactions, positions, and obligations, facilitating regulatory compliance and reporting obligations. By enforcing rules, standards, and best practices, ACS systems help ensure market integrity, protect investors, and maintain confidence in the financial system. Compliance with regulatory and legal frameworks is essential to foster trust and credibility among market participants, regulators, and other stakeholders.

Automated Clearing and Settlement (ACS) systems are driven by a set of objectives aimed at improving efficiency, reducing risks, enhancing liquidity, and promoting transparency and compliance in financial markets. By fulfilling these objectives, ACS systems play a vital role in promoting stability, integrity, and resilience in financial systems worldwide. Understanding the objectives of ACS systems is crucial for financial professionals, regulators, and policymakers seeking to foster innovation, efficiency, and integrity in clearing and settlement processes.

4.6 Need for Automated Clearing and Settlement Systems

Automated Clearing and Settlement (ACS) systems have emerged as essential infrastructure in modern financial markets, driven by a compelling need to address various challenges inherent in traditional manual processes. One primary need for ACS systems stems from the inefficiencies associated with manual clearing and settlement methods. Historically, these processes relied heavily on paper-based documentation, manual verification, and cumbersome reconciliation procedures. Such manual processes were prone to errors, delays, and increased operational costs, highlighting the urgent need for automation to streamline workflows and enhance efficiency.

Moreover, the increasing complexity and volume of transactions in financial markets necessitate the adoption of automated solutions for clearing and settlement. Manual processes struggle to cope with the sheer volume and speed of transactions, leading to bottlenecks, backlogs, and increased settlement risk. ACS systems leverage technology to automate key tasks such as trade matching, validation, and settlement, enabling rapid processing of transactions and reducing the time required to complete trades. Real-time processing capabilities further enhance efficiency by facilitating instantaneous validation and settlement, minimizing delays, and ensuring timely execution of transactions.

Another critical need for ACS systems lies in risk mitigation. Manual clearing and settlement processes are inherently susceptible to various risks, including operational errors, fraud, and settlement failures. These risks pose significant challenges to market participants, regulators, and other stakeholders, undermining market integrity and stability. ACS systems help mitigate these risks by automating processes, implementing robust risk management measures, and enhancing transparency. Real-time monitoring and surveillance tools enable early detection of anomalies or irregularities, allowing for prompt intervention and risk mitigation strategies, thereby safeguarding the integrity of financial markets.

Furthermore, ACS systems play a crucial role in improving liquidity and optimizing capital efficiency in financial markets. Traditional settlement methods often required participants to hold excess liquidity to cover settlement obligations, tying up capital that could otherwise be deployed more productively. By leveraging netting and optimization techniques, ACS systems minimize liquidity requirements and free up capital for other purposes. Real-time settlement capabilities enhance liquidity by accelerating the availability of funds and securities, enabling participants to deploy capital more efficiently and seize investment opportunities without delay.

Additionally, the need for transparency, compliance, and regulatory oversight in financial markets underscores the importance of ACS systems. Manual processes lack the transparency and audit trails necessary to track and monitor transactions effectively, making it challenging to enforce regulatory requirements and detect potential instances of market abuse or misconduct. ACS systems provide real-time visibility into transactions, positions, and obligations, facilitating regulatory compliance and reporting obligations. By enforcing rules, standards, and best practices, ACS systems help ensure market integrity, protect investors, and maintain confidence in the financial system.

The need for Automated Clearing and Settlement (ACS) systems arises from various challenges inherent in traditional manual processes, including inefficiencies, risks, and compliance issues. By addressing these needs, ACS systems play a vital role in enhancing efficiency, reducing risks, improving liquidity, and promoting transparency and compliance in financial markets. Understanding the need for ACS systems is essential for financial professionals, regulators, and policymakers seeking to foster innovation, efficiency, and integrity in clearing and settlement processes.

4.7 Benefits of Automated Clearing and Settlement Systems

1. Efficiency:

- ACS systems streamline processes, reduce operational costs, and improve operational efficiency.
- They enable faster transaction processing, shorter settlement cycles, and greater scalability to accommodate higher transaction volumes.

2. Risk Mitigation:

- ACS systems mitigate counterparty risk, settlement risk, and operational risk by automating processes and enhancing transparency.
- Real-time monitoring and surveillance tools help identify and address potential risks proactively.

3. Transparency and Compliance:

- ACS systems enhance transparency by providing real-time visibility into transactions, positions, and obligations.

- They facilitate regulatory compliance by enforcing rules, standards, and reporting requirements mandated by regulatory authorities.

4.8 Challenges and Considerations

1. Technology and Infrastructure:

- Implementing and maintaining ACS systems require robust technology infrastructure, including hardware, software, and network connectivity.
- Upgrades, cybersecurity threats, and interoperability issues pose ongoing challenges for ACS providers and participants.

2. Regulatory and Legal Frameworks:

- Compliance with regulatory requirements and legal frameworks governing clearing and settlement processes is essential.
- Changes in regulations, standards, and market practices may necessitate adjustments to ACS systems and procedures.

3. Operational Resilience:

- Maintaining operational resilience is critical to ensure the continuity of clearing and settlement operations.
- Business continuity planning, disaster recovery mechanisms, and cybersecurity measures are essential components of operational resilience.

Automated clearing and settlement systems play a pivotal role in modern financial markets, facilitating the efficient, secure, and timely completion of transactions. By leveraging technology to automate processes, mitigate risks, and enhance transparency, ACS systems contribute to the stability and integrity of financial systems worldwide. Understanding the key features, benefits, and challenges of ACS systems is essential for financial professionals, regulators, and policymakers seeking to navigate the evolving landscape of clearing and settlement.

4.9 Process of Automated Clearing and Settlement Systems

Automated Clearing and Settlement (ACS) systems streamline the complex processes involved in clearing and settling financial transactions through a series of well-defined steps. Understanding the process of ACS systems is crucial for financial professionals, regulators, and other stakeholders operating within the financial markets.

1. Trade Execution: The process begins with the execution of a trade, wherein buyers and sellers agree to exchange financial instruments such as stocks, bonds, or derivatives. This can occur on electronic trading platforms, stock exchanges, or over-the-counter (OTC) markets.

2. Trade Confirmation: Once a trade is executed, the details of the transaction are confirmed by both parties involved. This confirmation typically includes information such as the quantity, price, and terms of the trade.

3. Trade Matching: In ACS systems, trade details are electronically matched to ensure accuracy and consistency between the buyer's and seller's records. This step verifies that both parties agree on the terms of the trade before proceeding further.

4. Validation and Authorization: After trade matching, the transaction is validated and authorized by the relevant parties, including clearinghouses, central securities depositories

(CSDs), and financial institutions. This validation ensures that the trade complies with regulatory requirements and meets the necessary risk management criteria.

5. Netting: Netting involves offsetting transactions to reduce the overall amount of funds or securities that need to be exchanged. ACS systems leverage netting techniques to optimize liquidity, minimize settlement risk, and reduce the number of transactions processed. Netting can occur on a bilateral or multilateral basis, depending on the arrangement between counterparties.

6. Clearing: Once trades are validated and netted, the clearing process begins. Clearing involves the submission of transaction details to a clearinghouse or central counterparty (CCP), which acts as an intermediary between buyers and sellers. The clearinghouse verifies the authenticity of trades, calculates net positions, and determines the obligations of each participant.

7. Settlement Instruction: After clearing, settlement instructions are generated and transmitted to the relevant parties, instructing them to transfer funds and securities to fulfill their obligations. These instructions include details such as the amount, currency, and timing of settlement.

8. Settlement: The final step in the process is settlement, where funds and securities are exchanged between counterparties to fulfil their contractual obligations. Settlement can occur through various channels, including payment systems, securities depositories, and central banks. In ACS systems, settlement is often facilitated electronically in real-time or on a specified settlement date.

9. Post-Settlement Processing: Following settlement, post-settlement processing activities may occur, including reconciliation, confirmation, and reporting. These activities ensure that transactions are accurately recorded, and any discrepancies are promptly resolved.

Overall, the process of Automated Clearing and Settlement Systems involves a series of interconnected steps designed to ensure the efficient, timely, and secure completion of financial transactions. By leveraging automation, technology, and standardized processes, ACS systems contribute to the stability, integrity, and efficiency of financial markets worldwide.

4.10 Summary

Automated Clearing and Settlement Systems (ACSS) stand at the forefront of modern financial infrastructure, revolutionizing the way transactions are processed, cleared, and settled. A comprehensive understanding of ACSS entails recognizing its evolution, functions, and significance in facilitating efficient and secure payment operations within financial markets.

At its core, ACSS encompasses a range of electronic systems and processes designed to automate the clearing and settlement of financial transactions. These systems enable the seamless transfer of funds between financial institutions, ensuring timely and accurate settlement while minimizing operational risks. ACSS serves as the backbone of financial markets, facilitating various payment instruments, including checks, electronic funds transfers (EFTs), and securities transactions.

One of the key functions of ACSS is to streamline the clearing and settlement process, reducing the time and resources required to complete transactions. Traditionally, clearing involves the verification, netting, and reconciliation of transactions, while settlement involves the actual transfer of funds or securities between parties. ACSS automates these processes, accelerating transaction processing times and minimizing settlement risks, such as credit and liquidity risks.

Moreover, ACSS plays a crucial role in enhancing the efficiency and stability of financial markets. By automating clearing and settlement operations, ACSS helps mitigate operational risks associated with manual processes, such as errors, delays, and fraud. Additionally, the introduction of real-time settlement mechanisms, such as RTGS systems, minimizes settlement risks and enhances market liquidity, contributing to overall financial stability.

Looking ahead, the future of ACSS is likely to be shaped by ongoing technological innovations and regulatory developments. Emerging technologies, such as blockchain and distributed ledger systems, hold the potential to further streamline clearing and settlement processes, enhance transparency, and reduce counterparty risks. However, challenges such as interoperability, scalability, and regulatory compliance must be addressed to realize the full potential of these technologies in mainstream financial markets.

4.11 Keywords

Straight-Through Processing (STP):STP automates the end-to-end processing of transactions without manual intervention.It eliminates the need for rekeying data, reducing errors, and speeding up the settlement process.

Netting: Netting involves offsetting transactions to reduce the overall amount of funds or securities that need to be exchanged.Netting optimizes liquidity, reduces settlement risk, and minimizes the number of transactions processed.

Technology and Infrastructure: Implementing and maintaining ACS systems require robust technology infrastructure, including hardware, software, and network connectivity.Upgrades, cybersecurity threats, and interoperability issues pose ongoing challenges for ACS providers and participants.

Operational Resilience: Maintaining operational resilience is critical to ensure the continuity of clearing and settlement operations.Business continuity planning, disaster recovery mechanisms, and cybersecurity measures are essential components of operational resilience.

Settlement: The final step in the process is settlement, where funds and securities are exchanged between counterparties to fulfil their contractual obligations. Settlement can occur through various channels, including payment systems, securities depositories, and central banks. In ACS systems, settlement is often facilitated electronically in real-time or on a specified settlement date.

4.12 Self-Assessment Questions:

1. Define Automated Clearing and Settlement Systems (ACSS) and explain their significance in modern financial infrastructure.
2. How has technology influenced the evolution of ACSS over time?
3. What are the key functions of ACSS, and how do they contribute to the efficiency of financial markets?
4. Explain the difference between clearing and settlement in the context of ACSS.
5. What role do real-time gross settlement (RTGS) systems play in minimizing settlement risks?

6. Why is interoperability important in the context of ACSS, especially in the era of globalization?
7. How have international frameworks like the Continuous Linked Settlement (CLS) system addressed challenges in cross-border transactions?
8. Discuss the potential impact of emerging technologies such as blockchain on ACSS.
9. What are some of the challenges that ACSS may face in adopting new technologies and regulatory frameworks?
10. How does ACSS contribute to overall financial stability, and what are the implications of its efficient operation for the global economy?

4.13 Suggested Readings:

1. Peter Norman (2017). "Payment Systems: Design, Governance, and Oversight". Wiley
2. David Loader (2003). "Clearing, Settlement and Custody". Butterworth-Heinemann. Publications.
3. Ronald J. Mann and Jay Lawrence Westbrook (2016). "Payment Systems and Other Financial Transactions: Cases, Materials, and Problems". Aspen Publishers Publications.
4. John J. Kirton and Victor V. Ramraj (2012). "Central Banking and Financial Stability in East Asia". Routledge Publications.
5. Rodrigo Olivares-Caminal, Dalvinder Singh, and John Tribe (2019). "Digital Payments and Networks: Legal and Regulatory Challenges." Routledge Publications.

Dr. B. Sreedhar Reddy

Lesson- 5
REAL-TIME PROCESSING& STRAIGHT-THROUGH PROCESSING

Learning Objectives

- To Define Real-time Processing and Straight-Through Processing (STP)
- To Explore the technological infrastructure and components involved in Real-time Processing and STP
- To Analyze the benefits and challenges associated with Real-time Processing and STP
- To Best practices in governing Real-time Processing and STP

Structure

5.0 Introduction

Automated Clearing and Settlement Systems (ACSS) play a pivotal role in the modern financial ecosystem, facilitating the seamless transfer of funds between financial institutions. With the evolution of technology, real-time processing has emerged as a game-changer in enhancing the efficiency, speed, and reliability of these systems. In this article, we delve into the intricacies of real-time processing within ACSS, exploring its benefits, challenges, and the mechanisms involved.

Automated Clearing and Settlement Systems are infrastructure frameworks that enable the electronic transfer of funds between banks and other financial institutions. Traditionally, these systems operated on batch processing, where transactions were accumulated over a period and settled periodically, often daily or multiple times a day. While effective, batch processing had inherent limitations in terms of speed and responsiveness to the rapidly evolving financial landscape.

5.1 Real-Time Processing

Real-time processing within ACSS represents a paradigm shift from batch processing to instantaneous transaction settlement. Unlike batch processing, where transactions are grouped and settled periodically, real-time processing enables transactions to be processed and settled instantly, providing immediate access to funds and real-time updates on account balances.

5.1.1Benefits of Real-Time Processing:

1. Enhanced Speed and Efficiency: Real-time processing significantly reduces the time taken to settle transactions, enabling near-instantaneous fund transfers between financial institutions.
2. Improved Liquidity Management: Real-time access to funds allows financial institutions to manage liquidity more effectively, optimizing their cash flow and reducing the need for overnight borrowing.
3. Enhanced Customer Experience: Real-time processing provides customers with immediate access to funds and real-time updates on their account balances, enhancing their overall banking experience.
4. Mitigation of Settlement Risks: By settling transactions in real-time, the risk associated with delayed or failed settlements is minimized, enhancing the stability and reliability of the financial system.

5.1.2Challenges and Considerations:

While real-time processing offers numerous benefits, its implementation poses several challenges and considerations:
1. Technological Infrastructure: Real-time processing requires robust technological infrastructure capable of handling high volumes of transactions with minimal latency.
2. Security and Fraud Prevention: Real-time processing necessitates stringent security measures to safeguard against unauthorized access, fraud, and cyber threats.
3. Regulatory Compliance: Real-time processing must comply with regulatory requirements governing fund transfers, data privacy, and anti-money laundering (AML) measures.
4. Interoperability: Achieving interoperability between different ACSS and financial institutions is essential to ensure seamless fund transfers across various platforms and networks.

5.1.3 Mechanisms of Real-Time Processing:

Real-time processing within ACSS is enabled through the implementation of advanced technologies and protocols, including:
1. Immediate Payment Systems (IPS): IPS platforms facilitate real-time fund transfers between financial institutions, providing instant settlement and confirmation of transactions.
2. Real-Time Gross Settlement (RTGS): RTGS systems settle individual transactions on a gross basis in real-time, ensuring immediate and irrevocable transfer of funds between accounts.
3. Payment Gateways and APIs: Payment gateways and Application Programming Interfaces (APIs) enable seamless integration between financial institutions, allowing for real-time authorization and settlement of transactions.

Real-time processing represents a transformative advancement in the realm of Automated Clearing and Settlement Systems, offering unparalleled speed, efficiency, and reliability in fund transfers. While its implementation poses challenges, the benefits of real-time processing are undeniable, driving innovation and reshaping the future of financial transactions. As technology continues to evolve, real-time processing is poised to revolutionize the financial landscape, ushering in a new era of instantaneous and frictionless transactions.

5.2 Immediate Payment Systems (IPS)

Immediate Payment Systems (IPS) represent a revolutionary approach to fund transfers within the financial ecosystem, enabling near-instantaneous settlement of transactions between individuals, businesses, and financial institutions. IPS platforms facilitate real-time transfer of funds, providing immediate access to funds and enhancing the efficiency and convenience of payment processes. Let's delve deeper into the key features, benefits, and mechanisms of Immediate Payment Systems:

5.2.1 Key Features of Immediate Payment Systems:

1. Real-Time Settlement: IPS platforms settle transactions instantly, allowing funds to be transferred between accounts in a matter of seconds.

2. 24/7 Availability: Unlike traditional payment systems that operate within specific hours, IPS platforms are available round-the-clock, enabling users to initiate transactions at any time, including weekends and holidays.

3. Immediate Confirmation: IPS provides immediate confirmation of transaction completion, offering users real-time updates on their account balances and transaction status.

4. Broad Accessibility: IPS platforms are accessible across various channels, including online banking, mobile apps, and point-of-sale terminals, making them convenient for users across different demographics.

5. Enhanced Security: IPS systems employ robust security measures, such as encryption, authentication, and fraud detection, to safeguard against unauthorized access and fraudulent activities.

5.2.2 Benefits of Immediate Payment Systems:

1. Speed and Efficiency: IPS platforms offer unparalleled speed and efficiency in fund transfers, eliminating the delays associated with traditional payment systems.

2. Improved Cash Flow Management: Real-time access to funds enables businesses to manage their cash flow more effectively, optimizing liquidity and reducing reliance on credit facilities.

3. Enhanced Customer Experience: IPS enhances the overall customer experience by providing immediate access to funds and real-time transaction updates, thereby improving satisfaction and loyalty.

4. Cost Savings: IPS platforms can lead to cost savings for businesses by reducing the need for manual intervention, reconciliation, and exception handling associated with delayed settlements.

5. Support for Innovation: IPS fosters innovation in the financial industry by enabling the development of new payment services and business models that leverage real-time fund transfers.

5.2.3 Mechanisms of Immediate Payment Systems:

1. Instant Payment Clearing and Settlement Systems (IPCS): IPCS platforms facilitate real-time clearing and settlement of transactions between participating banks and financial institutions. These systems utilize advanced technologies and protocols to process transactions instantly and securely.

2. Centralized Payment Hubs: Some IPS platforms operate through centralized payment hubs that act as intermediaries between participating banks, facilitating real-time fund transfers and ensuring interoperability across different payment networks.

3. Interbank Payment Gateways: Interbank payment gateways provide a secure and standardized interface for interbank transactions, enabling seamless integration and communication between different financial institutions.

5.3 Real-time Gross Settlement System (RTGS)

Definition: RTGS is a payment system that enables instantaneous and irrevocable transfer of funds between banks or financial institutions on a gross basis. It settles transactions individually and in real-time, meaning each transaction is processed as soon as it is initiated without any delay.

Purpose: RTGS systems are crucial for large-value and time-sensitive transactions where immediate settlement and certainty of funds transfer are paramount. It helps in minimizing settlement risk, enhancing liquidity management, and facilitating efficient interbank payments.

5.3.1 Key Components of RTGS

1. Participants:

- Banks and financial institutions that are members of the RTGS network.
- They must maintain accounts with the central bank or another designated settlement institution to participate.

2. Central Infrastructure:

- Central bank or a designated authority operates the core infrastructure of the RTGS system.
- This infrastructure includes servers, communication networks, and security protocols to ensure smooth and secure transactions.

3. Payment Messages:

- Payments in RTGS are initiated through electronic payment messages such as SWIFT (Society for Worldwide Interbank Financial Telecommunication) messages.
- These messages contain essential information such as the sender's and receiver's identities, amount, and purpose of the transaction.

4. Settlement Process:

- Transactions in RTGS are settled on a gross basis, meaning each transaction is processed individually and settled immediately upon initiation.
- Funds transfer is irrevocable, ensuring that once a payment is made, it cannot be reversed.

5. Liquidity Management:

- RTGS systems typically incorporate liquidity management tools to ensure that participants maintain sufficient funds to settle their obligations.
- Central banks often provide liquidity support to ensure smooth functioning of the system, especially during periods of high transaction volumes or liquidity shortages.

5.3.2 Benefits of RTGS

1. Real-time Settlement:

RTGS enables instantaneous settlement of transactions, reducing counterparty risk and providing certainty of funds transfer.

2. Increased Efficiency:

By automating payment processing and settlement, RTGS improves efficiency and reduces operational costs for financial institutions.

3. Enhanced Security:

RTGS systems employ robust security measures to protect against fraud and unauthorized access, ensuring the safety of transactions.

4. Liquidity Optimization:
RTGS facilitates better liquidity management for banks, allowing them to optimize their cash flows and meet their payment obligations promptly.

5.3.3 Challenges and Considerations

1. High Costs:
Implementation and maintenance of RTGS systems can involve significant upfront costs and ongoing operational expenses.

2. Integration Complexity:
Integrating RTGS systems with existing banking infrastructure and legacy systems can be complex and time-consuming.

3. Regulatory Compliance:
RTGS systems must comply with regulatory requirements, including anti-money laundering (AML) and know-your-customer (KYC) regulations, adding to the complexity of implementation and operation.

4. Systemic Risk:
While RTGS systems mitigate counterparty risk at an individual level, they may introduce systemic risk if there are disruptions or failures in the central infrastructure.

5.4 Payment Gateways

Payment gateways and APIs (Application Programming Interfaces) are essential components of modern e-commerce and financial transactions, enabling seamless and secure processing of payments between merchants, customers, and financial institutions.

A payment gateway is a technology platform that facilitates the authorization and processing of online transactions, allowing merchants to accept payments from customers via various payment methods, including credit cards, debit cards, digital wallets, and bank transfers.

1. Transaction Processing: Payment gateways securely transmit transaction data between the merchant's website or point-of-sale system and the payment processor, encrypting sensitive information to prevent unauthorized access.

2. Payment Methods: Payment gateways support multiple payment methods, allowing customers to choose their preferred way of paying for goods or services. Common payment methods include credit/debit cards, e-wallets (e.g., PayPal, Apple Pay), bank transfers, and cryptocurrencies.

3. Security Features: Payment gateways implement robust security measures, such as encryption, tokenization, and fraud detection, to safeguard sensitive payment information and prevent fraudulent transactions.

4. Integration: Payment gateways offer integration options for merchants, including hosted payment pages, API integration, and plugins for popular e-commerce platforms like Shopify, WooCommerce, and Magento.

5. Settlement: After a transaction is authorized, the payment gateway facilitates the settlement process, transferring funds from the customer's account to the merchant's account, typically within a specified time frame.

5.5 APIs (Application Programming Interfaces)

APIs are sets of protocols, tools, and definitions that enable different software applications to communicate and interact with each other. In the context of payment processing, APIs play a crucial role in facilitating the integration of payment gateways with merchant websites, mobile apps, and point-of-sale systems.

1. Integration: Payment gateway APIs provide developers with standardized interfaces for integrating payment processing functionality into their applications. Developers can use APIs to send payment requests, receive responses, and handle various aspects of the payment lifecycle.

2. Customization: APIs offer flexibility for developers to customize the payment experience according to their specific requirements, such as implementing custom checkout flows, adding support for additional payment methods, or integrating with third-party services.

3. Real-Time Updates: Payment gateway APIs provide real-time updates on transaction status, allowing merchants to track payments, manage orders, and handle exceptions effectively.

4. Security: APIs implement security mechanisms, such as authentication, access controls, and data encryption, to ensure the confidentiality and integrity of payment data transmitted between systems.

5. Scalability: Payment gateway APIs are designed to handle high volumes of transactions efficiently, enabling merchants to scale their payment processing infrastructure as their business grows.

Payment gateways and APIs form the backbone of modern payment processing infrastructure, enabling merchants to accept payments securely and efficiently across various channels. By leveraging these technologies, businesses can streamline their payment processes, enhance the customer experience, and drive growth in e-commerce and digital payments.

5.6 Straight-Through Processing (STP)

Straight-Through Processing (STP) in Automated Clearing and Settlement Systems (ACSS) is a streamlined approach to transaction processing that aims to automate the entire lifecycle of a transaction, from initiation to settlement, without manual intervention or rekeying of data. STP enhances the efficiency, speed, and accuracy of transaction processing within ACSS, reducing operational costs, minimizing errors, and optimizing liquidity management. Let's delve deeper into the concept and mechanisms of Straight-Through Processing in ACSS:

5.6.1 Key Features of Straight-Through Processing (STP):

1. End-to-End Automation: STP automates the entire transaction lifecycle, including data capture, validation, authorization, clearing, and settlement, eliminating the need for manual intervention at each stage.

2. Real-Time Processing: STP enables real-time processing of transactions, allowing for instantaneous authorization, clearing, and settlement, thereby reducing transaction processing times and enhancing liquidity management.

3. Integration with Systems: STP systems are seamlessly integrated with internal and external systems, including payment gateways, core banking systems, and clearing and settlement networks, facilitating efficient data exchange and communication.

4. Error Handling and Exception Management: STP systems incorporate robust error handling mechanisms and exception management workflows to identify and resolve discrepancies or issues that may arise during transaction processing.

5. Compliance and Risk Management: STP systems adhere to regulatory requirements andrisk management protocols, including anti-money laundering (AML) regulations, know-your-customer (KYC) checks, and fraud detection mechanisms, to ensure the legality and security of transactions.

5.6.2 Benefits of Straight-Through Processing (STP) in ACSS:

1. Operational Efficiency: STP reduces manual processing efforts and administrative overheads, allowing financial institutions to streamline their operations and focus on value-added activities.

2. Cost Reduction: By automating transaction processing, STP reduces operational costs associated with manual data entry, reconciliation, and exception handling, leading to significant cost savings for financial institutions.

3. Improved Accuracy and Compliance: STP systems minimize errors and discrepancies in transaction processing, ensuring data accuracy and regulatory compliance, thereby mitigating operational and reputational risks

4.Enhanced Speed and Scalability: STP enables real-time processing of transactions, enhancing the speed and scalability of ACSS, and accommodating high transaction volumes efficiently.

5.Pptimized Liquidity Management: STP provides real-time visibility into cash flows and liquidity positions, enabling financial institutions to optimize liquidity management strategies and mitigate settlement risks effectively.

5.6.3 Mechanisms of Straight-Through Processing (STP) in ACSS:

1. Data Capture and Validation: Transaction data is captured electronically from various sources, such as online banking platforms, mobile apps, or point-of-sale terminals, and validated against predefined rules and criteria.

2. Automated Routing and Clearing: Validated transactions are automatically routed to the appropriate clearing and settlement networks based on predetermined criteria, such as transaction type, currency, and destination.

3. Real-Time Authorization and Settlement: Authorized transactions are settled in real-time, with funds transferred electronically between the accounts of the payer and payee, ensuring instantaneous availability of funds.

4. Exception Handling and Reconciliation: STP systems monitor transaction processing in real-time and identify exceptions or discrepancies, which are flagged for resolution through automated workflows or manual intervention, as necessary.

Straight-Through Processing (STP) in Automated Clearing and Settlement Systems (ACSS) represents a paradigm shift towards automated, efficient, and real-time transaction processing, offering numerous benefits in terms of operational efficiency, cost reduction, risk mitigation, and liquidity management. By leveraging STP technologies and mechanisms, financial institutions can optimize their transaction processing workflows, enhance customer experience, and stay competitive in the rapidly evolving financial landscape.

5.7 Net Settlement Systems

Definition: Net settlement systems are payment systems where multiple transactions between participants are aggregated or netted out to determine the final settlement amount. Unlike real-time gross settlement (RTGS) systems, net settlement systems settle transactions on a net basis rather than individually and in real-time.

Purpose: Net settlement systems are typically used for low-value and high-volume transactions, where the cost and operational efficiency of processing individual transactions in real-time may not be feasible. By netting out transactions, these systems reduce the number of payments required, thus minimizing processing costs and liquidity requirements.

5.7.1 Key Components of Net Settlement Systems

1. Participants:

- Similar to RTGS, net settlement systems involve banks and financial institutions as participants.
- Participants maintain accounts with the central clearing institution or another designated entity responsible for operating the net settlement system.

2. Central Infrastructure:

- A central clearing institution or a designated authority operates the core infrastructure of the net settlement system.
- This infrastructure includes databases, clearinghouses, and communication networks to process and settle transactions.

3. Clearing Process:

- Transactions submitted by participants are aggregated or netted out based on predefined rules or criteria.
- Netting can be done on a bilateral or multilateral basis, depending on the design of the net settlement system.
- Once netted, participants' obligations are calculated, and settlement instructions are generated for the final settlement process.

4. Final Settlement:

- After netting, participants settle their net obligations through a final settlement process.

- Settlement can occur through various means, including transfers of central bank reserves, commercial bank accounts, or other designated settlement assets.

5. Risk Management:

- Net settlement systems incorporate risk management mechanisms to mitigate credit and liquidity risks.
- Collateral requirements, participant credit limits, and monitoring mechanisms are often implemented to ensure the stability and safety of the system.

5.7.2 Benefits of Net Settlement Systems

1. Cost Efficiency:

By aggregating transactions and settling on a net basis, net settlement systems reduce the number of payments required, leading to lower processing costs for participants.

2. Reduced Liquidity Requirements:

Since transactions are netted out, participants' liquidity requirements are minimized compared to real-time gross settlement systems, where funds must be available for each transaction.

3. Operational Simplification:

Net settlement systems streamline payment processing and reconciliation by consolidating multiple transactions into a single settlement amount.

4. Scalability:

Net settlement systems can handle high volumes of transactions efficiently, making them suitable for processing large numbers of low-value payments.

5.7.3 Challenges and Considerations

1. Settlement Risk:

- While net settlement systems reduce liquidity requirements, they still entail settlement risk, particularly if participants fail to meet their obligations.
- Adequate risk management measures must be in place to address this risk effectively.

2. Timing Issues:

Unlike RTGS, where transactions are settled in real-time, net settlement systems may involve delays in final settlement, which could impact cash flow management for participants.

3. Systemic Risk:

Concentration of transactions and interconnectedness among participants in net settlement systems may pose systemic risks, particularly during periods of financial stress or operational disruptions.

4. Regulatory Compliance:

Net settlement systems must comply with regulatory requirements, including those related to risk management, transparency, and participant eligibility.

Net settlement systems play a vital role in processing high volumes of low-value transactions efficiently and cost-effectively.By aggregating transactions and settling on a net basis, these systems reduce processing costs and liquidity requirements for participants.However, effective risk management and regulatory compliance are essential to mitigate settlement risk and ensure the stability and integrity of net settlement systems within the broader financial system.

5.8 Summary

In this comprehensive lesson on Real-time Processing and Straight-Through Processing (STP), we delve into the dynamic realm of transaction processing in the financial industry. Real-time Processing, characterized by instantaneous transaction execution and settlement, and STP, which enables seamless end-to-end automation of transaction workflows, stand as pillars of efficiency and speed in modern financial operations. Through an exploration of their technological underpinnings, including data validation mechanisms, standardized message formats such as ISO 20022, and integration with external systems, learners gain insight into the intricate workflow and operational mechanics driving these processes. We meticulously dissect the myriad benefits, such as reduced operational costs, minimized errors, and enhanced risk management, juxtaposed with the challenges, including the need for robust cybersecurity measures and system resilience, inherent in Real-time Processing and STP. Moreover, we scrutinize the regulatory landscape and industry standards governing these processes, emphasizing compliance requirements, operational risk management guidelines, and the paramount importance of data privacy and security protocols in ensuring the integrity, transparency, and trustworthiness of real-time transaction processing systems. By navigating this multifaceted terrain, learners emerge equipped with a profound understanding of the transformative power of Real-time Processing and STP in reshaping the landscape of financial transactions and operations.

5.9 Keywords

Interoperability: Achieving interoperability between different ACSS and financial institutions is essential to ensure seamless fund transfers across various platforms and networks.

Immediate Payment Systems (IPS): IPS platforms facilitate real-time fund transfers between financial institutions, providing instant settlement and confirmation of transactions.

Real-Time Gross Settlement (RTGS): RTGS systems settle individual transactions on a gross basis in real-time, ensuring immediate and irrevocable transfer of funds between accounts.

Payment Gateways and APIs: Payment gateways and Application Programming Interfaces (APIs) enable seamless integration between financial institutions, allowing for real-time authorization and settlement of transactions.

Instant Payment Clearing and Settlement Systems (IPCS): IPCS platforms facilitate real-time clearing and settlement of transactions between participating banks and financial institutions. These systems utilize advanced technologies and protocols to process transactions instantly and securely.

5.10 Self-Assessment Questions

1. Define Real-time Processing and Straight-Through Processing (STP), and explain how they differ from traditional batch processing methods.
2. Describe the technological components involved in Real-time Processing and STP, including data validation mechanisms, message formats, and integration with external systems.
3. Discuss the benefits of Real-time Processing and STP, such as reduced operational costs, minimized errors, and enhanced risk management, and provide examples of how they improve efficiency in financial transactions.

4. Identify potential challenges associated with implementing Real-time Processing and STP, including cybersecurity vulnerabilities, system resilience, and regulatory compliance requirements.
5. Explain the role of regulatory frameworks and industry standards in governing Real-time Processing and STP, and discuss the importance of compliance with data privacy and security protocols.
6. Reflect on the implications of Real-time Processing and STP for financial institutions and markets, considering factors such as customer experience, operational efficiency, and the evolution of transaction processing technologies.

5.11 Suggested Readings

1. Ayesha Khanna (2011). Straight Through Processing for Financial Services: The Complete Guide. Palgrave Macmillan
2. Phillip A. Laplante (2011). Real-Time Systems Design and Analysis: Tools for the Practitioner. John Wiley & Sons
3. Hermann Kopetz (2011). Real-Time Systems: Design Principles for Distributed Embedded Applications. Springer
4. Bhavesh Patel (2007). Straight Through Processing (STP): The Route to Integrated Processing. Global Professional Publishing
5. Byron Ellis (2014). Real-Time Analytics: Techniques to Analyze and Visualize Streaming Data. Wiley
6. L. Cooper (2007). Straight Through Processing (STP): A Case Study. AuthorHouse.

Dr. B. Sreedhar Reddy

Lesson- 6

GLOBAL SETTLEMENT NETWORKS: A COMPREHENSIVE OVERVIEW

Learning Objectives

- To Define global settlement networks and elucidate their role in facilitating cross-border financial transactions
- To Explore the structure and operation of global settlement networks
- To Analyze the benefits and challenges associated with global settlement networks
- To Evaluate the role of regulatory frameworks, industry standards, and international cooperation in governing global settlement networks

Structure

6.0 Introduction

Global Settlement Networks are vital infrastructure systems that facilitate the seamless transfer of funds and settlement of financial transactions across borders. Understanding these networks is crucial for students studying finance, economics, international business, or related fields. This comprehensive overview aims to provide students with a clear understanding of global settlement networks, their significance, key players, and how they contribute to the functioning of the global financial system.

6.1 Global Settlement Networks

Global Settlement Networks are infrastructure frameworks that enable the settlement of financial transactions between banks and financial institutions located in different countries. These networks provide the necessary infrastructure and protocols for the transfer of funds, ensuring that transactions are processed efficiently, securely, and in compliance with relevant regulations.

6.1.1 Significance of Global Settlement Networks

1. Facilitating International Trade: Global settlement networks facilitate cross-border trade by enabling the transfer of funds between buyers and sellers in different countries, thereby supporting global commerce.

2. Promoting Financial Integration: These networks contribute to the integration of global financial markets by providing mechanisms for the transfer and settlement of financial assets, such as currencies, securities, and derivatives.

3. Reducing Settlement Risk: By providing real-time or near-real-time settlement of transactions, global settlement networks help reduce settlement risk and counterparty risk, enhancing the stability and resilience of the financial system.

4. Supporting Economic Growth: Efficient settlement networks support economic growth and development by facilitating capital flows, investment, and access to financial services on a global scale.

6.1.2 Key Players in Global Settlement Networks

1. SWIFT (Society for Worldwide Interbank Financial Telecommunication): SWIFT is a leading provider of messaging services and standards for global financial transactions, connecting thousands of banks and financial institutions worldwide.

2. CHIPS (Clearing House Interbank Payments System): CHIPS is a major settlement network in the United States, providing real-time settlement of high-value transactions denominated in U.S. dollars.

3. TARGET2 (Trans-European Automated Real-time Gross Settlement Express Transfer System): TARGET2 is the RTGS system for the euro, operated by the Eurosystem, facilitating the settlement of euro-denominated payments within the European Union.

4. SEPA (Single Euro Payments Area): SEPA is an initiative aimed at harmonizing payment systems within the eurozone, enabling cross-border euro payments under uniform standards and rules.

5. CLS (Continuous Linked Settlement): CLS specializes in the settlement of foreign exchange transactions, providing simultaneous settlement of both legs of an FX trade to mitigate settlement risk.

6.1.3 Process of Global Settlement Networks

1. Transaction Initiation: A financial transaction is initiated by a sender, such as a business or individual, who instructs their bank to transfer funds to a recipient in another country.

2. Message Transmission: The sender's bank transmits payment instructions to the recipient's bank through a secure messaging network, such as SWIFT.

3. Clearing and Settlement: The recipient's bank processes the payment instructions, verifies the funds, and initiates the settlement process through the relevant settlement network, such as TARGET2 or CHIPS.

4. Funds Transfer: The settlement network facilitates the transfer of funds between the sender's bank and the recipient's bank in real-time or near-real-time, ensuring the completion of the transaction.

5. Confirmation: Once the transaction is settled, confirmation messages are sent to both the sender and recipient, providing assurance that the funds have been transferred successfully.

Global Settlement Networks are essential infrastructure systems that underpin the functioning of the global financial system. By enabling the efficient, secure, and reliable settlement of financial transactions across borders, these networks support international trade, financial integration, and economic growth on a global scale. Students studying finance, economics, or international business can benefit from understanding the role and significance of global settlement networks in the modern world of finance.

6.2 SWIFT (Society for Worldwide Interbank Financial Telecommunication)

SWIFT is a cooperative organization founded in 1973, headquartered in Belgium. It operates a secure messaging network that connects thousands of banks and financial institutions worldwide. The primary purpose of SWIFT is to facilitate the exchange of financial messages between institutions, enabling them to conduct various transactions securely and efficiently.

6.2.1 Key Functions of SWIFT:

1. Messaging Services: SWIFT provides a platform for banks to exchange standardized financial messages, such as payment instructions, trade confirmations, and securities transactions. These messages follow specific formats defined by SWIFT, ensuring consistency and interoperability across the network.

2. Standardization: SWIFT establishes and maintains standardized message formats, known as SWIFT MT messages, which enable seamless communication between financial institutions. Standardization helps reduce errors, improve efficiency, and facilitate automation of processes.

3. Network Connectivity: SWIFT operates a secure network infrastructure that connects banks and financial institutions worldwide. The SWIFT network employs advanced security measures to protect the confidentiality and integrity of transmitted messages, ensuring trust and reliability.

4. Compliance and Security Services: SWIFT offers compliance and security services to help institutions adhere to regulatory requirements, combat financial crime, and mitigate operational risks. These services include sanctions screening, anti-money laundering (AML) controls, and cybersecurity measures.

6.2.2 Importance of SWIFT:

1. Global Connectivity: SWIFT connects thousands of financial institutions across the globe, enabling them to communicate and transact with each other seamlessly. This global connectivity is essential for facilitating cross-border payments, trade finance, and other international transactions.

2. Efficiency and Standardization: SWIFT's standardized messaging formats and network infrastructure promote efficiency, consistency, and automation in financial transactions. Institutions can rely on SWIFT to exchange messages quickly and accurately, reducing manual errors and processing times.

3. Security and Trust: The SWIFT network prioritizes security and trust, implementing robust encryption, authentication, and authorization mechanisms to protect sensitive financial information. Institutions trust SWIFT to transmit their messages securely, safeguarding against cyber threats and fraud.

4. Regulatory Compliance: SWIFT helps institutions comply with regulatory requirements by offering compliance services and tools. Institutions can use SWIFT's solutions to screen transactions for sanctions violations, conduct due diligence on counterparties, and report suspicious activities to regulatory authorities.

6.2.3 Impact of SWIFT on the Financial Industry:

1. Facilitating International Trade: SWIFT plays a vital role in facilitating international trade by enabling banks to process trade finance transactions, such as letters of credit and documentary collections, efficiently and securely.

2. Enabling Cross-Border Payments: SWIFT facilitates cross-border payments by providing a reliable and standardized platform for banks to exchange payment instructions. Institutions rely on SWIFT to settle payments in different currencies across the globe.

3. Supporting Securities Transactions: SWIFT supports the processing of securities transactions, such as trade confirmations, settlement instructions, and corporate actions notifications. Financial institutions use SWIFT to communicate and settle securities transactions efficiently.

4. Promoting Financial Inclusion: SWIFT's global network extends access to financial services and markets, enabling institutions in emerging economies to connect with the global financial system. This promotes financial inclusion and economic development worldwide.

SWIFT plays a central role in the global financial system, facilitating secure, efficient, and standardized communication and exchange of financial messages between institutions worldwide. Students studying finance, economics, or banking can benefit from understanding SWIFT's functions, importance, and impact on the financial industry, as it shapes the way international transactions are conducted and financial markets operate globally.

6.3 CHIPS (Clearing House Interbank Payments System)

CHIPS is an electronic payment system operated by The Clearing House, a banking association representing major U.S. banks. Established in 1970, CHIPS facilitates the settlement of high-value and time-sensitive payments between financial institutions in the United States.

6.3.1 Key Functions of CHIPS:

1. Real-Time Gross Settlement (RTGS): CHIPS operates as a real-time gross settlement (RTGS) system, meaning that each payment is settled individually and immediately upon submission. This ensures the immediate and irrevocable transfer of funds between participating banks.

2. High-Value Payments: CHIPS specializes in the settlement of high-value payments, typically involving large sums of money, such as corporate payments, interbank transfers, securities transactions, and other wholesale funds transfers.

3. Liquidity Management: CHIPS helps financial institutions manage their liquidity effectively by providing real-time settlement of payments. Banks can settle their obligations promptly, optimize their cash flows, and minimize the need for costly intraday borrowing.

4. Risk Mitigation: CHIPS reduces settlement risk and counterparty risk by settling transactions in real-time. This mitigates the risk of delayed or failed payments, enhancing the stability and resilience of the financial system.

6.3.2 Significance of CHIPS:

1. Efficient Payment Processing: CHIPS enables financial institutions to settle high-value payments quickly and securely, supporting the efficient functioning of financial markets and payment systems in the United States.

2. Systemic Importance: As one of the largest RTGS systems in the world, CHIPS plays a critical role in the U.S. financial system. It processes trillions of dollars in payments daily, facilitating the smooth flow of funds between banks and other financial institutions.

3. Interbank Connectivity: CHIPS fosters interbank connectivity by providing a centralized platform for banks to exchange high-value payments. This promotes collaboration and cooperation among financial institutions, enhancing the efficiency and stability of the banking sector.

4. Enhanced Liquidity Management: CHIPS helps banks optimize their liquidity management strategies by providing real-time settlement of payments. Banks can manage their liquidity positions more effectively, reducing the need for costly liquidity buffers and intraday borrowing.

6.3.3 Step by Step Process of CHIPS

1. Payment Submission: Financial institutions submit payment instructions to CHIPS electronically, indicating the amount, currency, and beneficiary details of each payment.

2. Real-Time Settlement: CHIPS processes each payment individually and settles it in real-time, ensuring immediate transfer of funds between the accounts of the sending and receiving banks.

3. Confirmation and Reporting: Once a payment is settled, CHIPS provides confirmation messages to the participating banks, indicating the completion of the transaction. Banks can also access reports and statements to reconcile their payment activities.

4. Continuous Operations: CHIPS operates continuously throughout the business day, allowing financial institutions to submit and settle payments in real-time, including during weekends and holidays.

CHIPS is a critical component of the U.S. financial infrastructure, providing real-time settlement of high-value payments between financial institutions. Students studying finance, economics, or banking can benefit from understanding CHIPS' functions, significance, and role in the U.S. payment system, as it shapes the way high-value payments are processed and settled in the United States.

6.4 Fedwire

Fedwire is a real-time gross settlement (RTGS) system operated by the Federal Reserve Banks. It facilitates the electronic transfer of funds and securities between participants, including banks, financial institutions, government agencies, and certain international organizations. Fedwire is widely used for high-value, time-sensitive payments, such as interbank transfers, securities transactions, and large-value corporate payments.

6.4.1 Key Functions of Fedwire:

1. Real-Time Gross Settlement (RTGS): Fedwire settles transactions on a real-time gross basis, meaning that each payment is settled individually and immediately upon submission. This ensures the immediate and irrevocable transfer of funds between participating banks.

2. High-Value Payments: Fedwire specializes in the settlement of high-value payments, typically involving large sums of money. It is used for various transactions, including interbank transfers, securities and Treasury transactions, corporate payments, and Federal Reserve transactions.

3. Systemic Importance: Fedwire is one of the largest RTGS systems globally and plays a critical role in the U.S. financial system. It processes trillions of dollars in payments daily, facilitating the smooth flow of funds between financial institutions and supporting the functioning of financial markets.

4. Liquidity Management: Fedwire helps financial institutions manage their liquidity effectively by providing real-time settlement of payments. Banks can settle their obligations promptly, optimize their cash flows, and minimize the need for costly intraday borrowing.

6.4.2 Significance of Fedwire:

1. Efficient Payment Processing: Fedwire enables financial institutions to settle high-value payments quickly and securely, supporting the efficient functioning of financial markets and payment systems in the United States.

2. Systemic Stability: Fedwire enhances the stability and resilience of the financial system by providing real-time settlement of payments. This helps reduce settlement risk and counterparty risk, mitigating the potential impact of disruptions or failures in the payment system.

3. Interbank Connectivity: Fedwire fosters interbank connectivity by providing a centralized platform for banks to exchange high-value payments. This promotes collaboration and cooperation among financial institutions, enhancing the efficiency and stability of the banking sector.

4. Facilitating Monetary Policy: Fedwire plays a crucial role in the implementation of monetary policy by the Federal Reserve. It allows the Federal Reserve to conduct open market operations, manage its balance sheet, and provide liquidity to financial markets efficiently.

6.4.3 Operational Framework of Fedwire:

1. Participant Access: Financial institutions that meet certain eligibility criteria, including membership in the Federal Reserve System and compliance with regulatory requirements, can become participants in Fedwire.

2. Payment Submission: Participants submit payment instructions to Fedwire electronically, indicating the amount, currency, and beneficiary details of each payment.

3. Real-Time Settlement: Fedwire processes each payment individually and settles it in real-time, ensuring immediate transfer of funds between the accounts of the sending and receiving banks.

4. Confirmation and Reporting: Once a payment is settled, Fedwire provides confirmation messages to the participating banks, indicating the completion of the transaction. Banks can also access reports and statements to reconcile their payment activities.

Fedwire is a critical component of the U.S. financial infrastructure, providing real-time settlement of high-value payments between financial institutions. MBA students studying finance, economics, or banking can benefit from understanding Fedwire's functions, significance, operational framework, and impact on the financial industry, as it shapes the way high-value payments are processed and settled in the United States.

6.5 Summary

In this comprehensive lesson on "Global Settlement Networks: A Comprehensive Overview," we embark on a detailed exploration of the intricate webs of connectivity that underpin cross-border financial transactions. Delving into the core principles and operational frameworks of global settlement networks, we unravel the complexities of correspondent banking relationships, clearing and settlement mechanisms, and messaging protocols such as SWIFT. Through meticulous analysis, learners gain a nuanced understanding of the pivotal role these networks play in facilitating international finance and trade, while grappling with the multifaceted challenges posed by regulatory compliance, financial crime prevention, and systemic risks. By navigating this comprehensive overview, students emerge equipped with the knowledge and insights needed to navigate the evolving landscape of global settlement networks with confidence and acumen.

6.6 Keywords

Global Settlement Networks: Global Settlement Networks are infrastructure frameworks that enable the settlement of financial transactions between banks and financial institutions located in different countries.
SWIFT (Society for Worldwide Interbank Financial Telecommunication): SWIFT is a leading provider of messaging services and standards for global financial transactions, connecting thousands of banks and financial institutions worldwide.
CHIPS (Clearing House Interbank Payments System): CHIPS is a major settlement network in the United States, providing real-time settlement of high-value transactions denominated in U.S. dollars.
Fedwire: Fedwire is a real-time gross settlement (RTGS) system operated by the Federal Reserve Banks. It facilitates the electronic transfer of funds and securities between participants, including banks, financial institutions, government agencies, and certain international organizations.
Liquidity Management: Fedwire helps financial institutions manage their liquidity effectively by providing real-time settlement of payments. Banks can settle their obligations promptly, optimize their cash flows, and minimize the need for costly intraday borrowing.

6.7 Self-Assessment Questions

1. Define global settlement networks and explain their significance in facilitating cross-border financial transactions. How do they differ from domestic settlement systems?
2. Describe the key components of global settlement networks, including correspondent banking relationships, clearing and settlement mechanisms, and messaging protocols like SWIFT. How do these components work together to facilitate international transactions?
3. What are some benefits of global settlement networks, and how do they contribute to increased efficiency, reduced settlement times, and enhanced liquidity management in international finance and trade?
4. Identify challenges associated with global settlement networks, such as regulatory compliance, financial crime prevention, and systemic risks. How can these challenges impact the integrity and stability of cross-border settlement systems?

5. Discuss the role of regulatory frameworks, industry standards, and international cooperation in governing global settlement networks. How do initiatives like the Financial Action Task Force (FATF) and Basel Committee on Banking Supervision (BCBS) contribute to ensuring the integrity and resilience of cross-border settlement systems?
6. Reflect on the implications of global settlement networks for financial institutions, businesses, and economies. How can stakeholders navigate the complexities and risks inherent in cross-border transactions to foster global financial stability and economic growth?

6.8 Suggested Readings

1. Youssef Cassis (2019). Cross-Border Payments and Settlements: An Introduction. Palgrave Macmillan
2. Steven J. Hanna (2016). International Payments, Clearing, and Settlement: A Guide to the Payments Network. Wiley
3. Dean Caire (2018). Global Banking and Payment Systems. Routledge
4. Charles H. Camp and Steven L. Schwarcz (2015). The Law of Global Payment Systems. Wolters Kluwer
5. Ralph Nader (2017). Payment Systems: From the Salt Mines to the Board Room. Bloomsbury Publishing
6. David Loader (2020). Clearing, Settlement, and Custody. Wiley

Dr. B. Sreedhar Reddy

Lesson-7
CRYPTOGRAPHIC METHODS FOR E-PAYMENT SECURITY

After reading this lesson, you will be able to understand:

Objectives:

- To understand the Cryptographic Method of E-Payment Security
- To discuss the Purpose and Benefits of Encryption in E-payments.
- To understand the Security and Risks of E-Payment System
- To understand the various Key Security Measures Behind Digital Payment Systems
- To understand the Online Payment Security.

Structure:

7.1. Introduction:

In recent years E-shopping gained a tremendous growth due to its benefits. Even though benefits of E-shopping are considerable, it creates some security threats such as debit, credit card fraud, phishing etc. In this paper we introduce an E-payment system that provides an unrivaled security using visual and quantum cryptography. Visual cryptography hides the details of customer by generating shares whereas Quantum cryptography secures the transmission of one-time password. Image steganography embeds the share with one time password which results in secure transmission of share to bank. Proposed approach guarantees unconditional security than traditional E-payment system by using two important cryptographic techniques.

In an increasingly digital world, the way we handle our finances has evolved significantly. From traditional cash transactions to checks and credit cards, the financial landscape has now embraced the convenience of digital payment systems. These systems have revolutionized how we conduct transactions and introduced a complex web of security measures to protect a financial asset of a business. Understanding these security measures is paramount in ensuring the safety of our digital financial interactions. There are many approaches to privacy and security.

Brief History: The web has emerged as the most dynamic force in the Information Technology (IT) industry during the past decade. This growth has been facilitated by the confluence of increasingly powerful and inexpensive technologies that permitted large-scale usage and the provision of scalable systems and applications, allied with the growing availability of telecommunications due to declining costs and increasing bandwidth thereby allowing the spread of digital information.

7.2. Meaning of Cryptographic Method of E-Payment Security:

The word "cryptography" is derived from the Greek kryptos, meaning hidden. The prefix "crypt-" means "hidden" or "vault," and the suffix "-graphy" stands for "writing. .Cryptography ensures confidentiality by encrypting sent messages using an algorithm with a key only known to the sender and recipient. Cryptography is the method of transforming data represented as unreadable binary numbers. Modern cryptographic methods are mathematical and are based on mathematical functions (modulo function, prime numbers, factoring large numbers, and permutations). Visual cryptography hides the details of customer by generating shares whereas Quantum cryptography secures the transmission of one-timepassword. Image steganography embeds the share with one time password which results in secure transmission of share to bank.

Secure payment cryptography, at its core, is like a secret handshake between your computer or smartphone and the payment gateway. It's a method of scrambling data—like your credit card information—so that only the intended recipient, the payment gateway, can understand it. This process helps protect your sensitive information from being intercepted or tampered with during transmission.

7.3. Importance of Cryptography:

Confidentiality is necessary for maintaining the privacy of those whose personal information is stored in enterprise systems. Encryption, therefore, is the only way to ensure that your information remains secure while it's stored and being transmitted. A secure payment system will facilitate the transfer of payment information and customer data, and provide protection against fraud and other potential safety issues.

The Importance of Encryption in Online Payment Services are:

i. **Data Privacy:** Encryption safeguards the privacy of sensitive data, preventing unauthorized access and protecting individuals from identity theft and fraud. It ensures that payment information, including credit card numbers, bank account details, and personal identification, remains confidential and inaccessible to cybercriminals.

ii. **Secure Transactions:** Encryption provides end-to-end security for online transactions. When a user initiates a payment, the payment information is encrypted before transmission. This means that even if a hacker manages to intercept the data during transmission, they would only see an unintelligible string of characters.

iii. **Mitigating Cyber Threats:** Cyberattacks, including phishing and man-in-the-middle attacks, pose significant threats to online payment services. Encryption adds a layer of protection against these threats by making it incredibly challenging for attackers to extract usable data from intercepted transmissions.

iv. **Regulatory Compliance:** Many regulatory standards, such as the Payment Card Industry Data Security Standard (PCI DSS), mandate the use of encryption to protect payment data. Compliance with these standards is essential for online payment services to ensure the security and trust of their users.

v. **Trust and Reputation:** Implementing strong encryption measures enhances the trustworthiness and reputation of online payment services. Users are more likely to engage with platforms that prioritize their security, leading to increased adoption and customer loyalty.

7.4.Purpose and Benefits of Encryption in E-payments:

Encryption is a process of transforming data into a secret code that only authorized parties can access and decipher. It is widely used in payment systems to protect sensitive information such as card numbers, PINs, passwords, and transaction details from hackers, fraudsters, and identity thieves.

i. Benefits to Business:

Greenstein and Feinman (2000) identify potential benefits to business which include:

a) Internet and web-based electronic commerce is more affordable and hence allows more business partners to be reached than with traditional electronic data interchange (EDI).
b) A geographically dispersed customer base is available
c) Procurement processing and purchasing costs can be lowered
d) Reduction in inventories with lower cycle times and
e) Better customer services with lower marketing and sales costs.

ii. Benefits to Consumers:

Consumers benefit in a number of ways such as:

a) Increased choice of vendors and products
b) Convenience coupled with competitive prices and increased price comparison capabilities
c) Greater amounts of information that can be accessed on demand.
d) Customization in the delivery of services.

iii. Web Security:

While technology can deliver innumerable benefits, it introduces new vulnerabilities that can be exploited by persons with the necessary technical skills. Hackers represent a well-known threat, but increasingly other criminal elements must be taken into consideration. An international survey carried out in 1998 reported that 73% of all companies reported some security breach or corporate espionage during the previous 12 months. Companies carrying out their business electronically were significantly more likely to be victims of security loss that affected their revenues and corporate data than traditional businesses (Information Week, 1998). The joint annual study between the Computer Security Institute (CSI) and the Federal Bureau of Investigation (FBI) has shown that verifiable losses in 1999 soared to $265.6 million, more than double the total reported for the three years 1996 to 1998 inclusive. Over 90% of respondents had detected some form of security attack on their computer systems during the year– denial of service (32%), sabotage of data or networks (19%), financial fraud (14%), insider abuse of Internet access privileges (97%), virus contamination (90%),. While outside intruders are perceived by the world to be the largest threat to security, FBI studies have revealed that 80% of intrusions and attacks come from within organizations (Price, 1999). An insider is someone who has been (explicitly or implicitly) granted privileges that authorize them to use a particular system of facility. Insider misuse involves misuse of authorized privileges. Insiders may have better knowledge of system vulnerabilities and the whereabouts of sensitive information. Nonetheless, to understand the security threats involved in using the Internet for communications, it is essential to understand that there are threats evident at different parts of the infrastructure used for electronic commerce.

iv. Payment Gateways:

A payment gateway is a software application that encrypts financial data and authorizes transactions, communicating with payment processors to enable the transfer of funds from buyer to seller.

Unless a business plan to run payment data through the business own servers — and make the significant investment it takes to do so safely — a business need a payment gateway, whether it's built into your hosting platform or incorporated via a third-party plug-in.

Payment gateway providers handle financial identifiers on behalf of their customers, protecting site owners from the risks associated with storing data on their own servers. Established gateways like PayPal and Authorize.Net invest heavily in security, charging membership and/or transaction fees to site operators.

7.5. Security and Risks of E-Payment System:

Despite strong security measures, electronic payment systems are vulnerable to hacking, data breaches, and identity theft, potentially exposing customers' sensitive information.

7.6. Ensuring Security in E-Payment:

Consider the following online payment security best practices to protect your customers and business.

i. Use two-factor authentication
ii. Verify every transaction
iii. Choose a secure e-commerce platform and payment provider
iv. Buy cyber liability insurance
v. Use a personal verification system
vi. Don't store customer payment data

7.7.Key Security Measures Behind Digital Payment Systems:

The following are the key security measures behind digital payment system:

i. **Encryption:** Encryption is a vital security measure in digital payment systems. It is a process of scrambling data so that it can only be read by someone with the correct decryption key. This helps to protect sensitive information from being intercepted by unauthorized parties. It protects sensitive information, ensures confidentiality, complies with industry standards, and builds trust with customers. By implementing encryption, digital payment systems can provide a safe and secure way to make transactions.

ii. **Authentication**: Authentication is the process of verifying the identity of a user, It protects sensitive information, ensures confidentiality, complies with industry standards, and builds trust with customers. Digital payment systems use various authentication methods, such as passwords, biometrics, and two-factor authentication, to ensure that only authorized users can access the system.

iii. **Two-factor authentication (2FA):** 2FA is a security measure that requires users to provide two forms of identification in order to complete a transaction. This typically involves entering a password or PIN, as well as a code that is sent to the user's phone.

iv. **Authorization:** Authorization is the process of granting access to specific resources or actions. Digital payment systems use authorization to ensure that only authorized users can perform specific actions, such as making a payment or accessing account information.

v. **Tokenization:** Tokenization is a process of replacing sensitive data with a unique identifier, or token. This token can then be used to process transactions without revealing the underlying data.

vi. **Biometrics:** Many digital payment systems now incorporate biometric authentication, such as fingerprint or facial recognition. Biometrics provide a highly secure way to verify a user's identity, as they are difficult to replicate.

vii. **Email Validation and Authentication:** Payment service providers can use email validation and authentication to detect and prevent email phishing and spoofing early on. This measure can help prevent unauthorized access to user accounts

viii. **Two-factor authentication (2FA):** 2FA is a security measure that requires users to provide two forms of identification in order to complete a transaction. This typically involves entering a password or PIN, as well as a code that is sent to the user's phone.

ix. **Secure Socket Layer (SSL) and Transport Layer Security (TLS):** These protocols establish secure connections between a user's device and a payment system's server. SSL and TLS ensure that data transmitted during a transaction is secure and cannot be intercepted by malicious actors.

7.8. Online Payment Security Methods:

Online Payment security refers to the processes and practices used to safeguard financial transactions, funds and personal information of clients from threats like online payment fraud, unauthorized access, and data breaches.If a customer's data and money are compromised, your company may be subject to legal and financial consequences. To avoid this, you must use a secure payment system for your business.

11 best practices that business can use to establish a robust mechanism to Secure Online Payment Processing are:

i. Implementing data encryption.
ii. Observing PCI-DSS compliance, a set of rules developed by the PCI Security Standards Council.
iii. Using 3D Secure, a method used to implement payment security in e-commerce to verify a customer's identity.
iv. Choosing a safe platform and payment gateway.
v. Keeping your operating systems updated.
vi. Implementing payment tokenization.
vii. Enabling two-factor authentication.

viii. Verifying transaction details, like CVV, billing address, phone number and email ID, before allowing an online payment.
ix. Fraud prevention and monitoring systems.
x. Training your staff on data protection guidelines and security measures.
xi. Explaining security measures to customers.

11 Best Practices for Secure Online Payment Processing are:

i. Data Encryption (TLS & SSL Protocols):
Data encryption is the process of encoding the payment information so that only the person who holds the encryption key can decode it. The data is encrypted to provide end-to-end protection.

TLS (Transport Layer Security) and SSL (Secure Sockets Layer) are two key protocols that are used to encrypt data.

SSL is an internet security protocol based on encryption. It was developed in 1995 to guarantee data integrity, privacy and authenticity in online communications.

TLS is a cryptographic security protocol that emerged from SSL and is used to preserve data integrity and anonymity for communications over the Internet. Its most widely-known use is for securing HTTPS. Without TLS encryption in place, all data sent over the Internet is unencrypted and is visible to anyone with the means and intent to intercept it.

An easy way to check if the e-commerce websites you frequent are SSL-certified is to look at the URL and see if they use the “http://” or the “https://” protocol. The additional ‘s’ signifies a secure e-payment system. You can also look for the padlock icon at the beginning of the URL. Modern web browsers, in their race to make the Web secure by default, are marking HTTP sites as ‘insecure’.

The more recent protocol, TLS, can be considered an upgrade to SSL. Compared to SSL, TLS is easier to use, more dependable, and offers more security. SSL is less prevalent than TLS.

ii. PCI-DSS Compliance:
The PCI Security Standards Council is a global organization that maintains and promotes compliance rules for managing cardholder data for all e-commerce websites and online payment systems.

The Payment Card Industry Data Security Standards (PCI-DSS) is, in effect, a set of policies that govern how sensitive cardholder information should be handled.

Fact: The PCI Security Standards Council was created as a joint initiative by the four major credit-card providers: American Express, Visa, MasterCard, and Discover, in the year 2004. Over the years, the PCI-DSS standard has become the guiding principle for online security across the globe.

For an e-commerce website or an online payment system to be PCI-DSS compliant, they have to follow certain directives:

- Maintain a secure network to process payments
- Use robust firewalls to safeguard your website from malicious security threats.
- Make sure your payment gateway or website does not use default credentials, like PINs or passwords provided by the manufacturer.
- Allow customers to change their credentials whenever necessary on your website or payment gateway.
- Ensure all data is encrypted during transmission
- The cardholder data should be encrypted before it is transferred online. Razorpay encrypts all information you share using checkout via TLS. This prevents data interception during transmission from your system to Razorpay.

Keep infrastructure secure
This directive involves –

- Staying aware of new PCI-DSS mandates.
- Using updated software and spyware to protect against known software vulnerabilities.
- Running regular system and software scans to provide maximum data protection.
- Restrict information access
- Cardholder data must be protected at all times, both electronically and physically.

E--Commerce websites must restrict access to confidential information so that only authorized personnel can access cardholder data.

iii. 3D Secure:
3D Secure is used to maintain payment security in e-commerce by verifying a customer’s identity. It serves as an extra layer of authentication during the online checkout process and is administered by the cardholder’s bank.

3D Secure is implemented to prevent the unauthorized use of cards. It can include biometric scans or entering PIN codes to verify the cardholder’s identity.

The many advantages of 3D Secure are as follows –

- Reduced risk of online payment fraud
- Enhanced protection of customer data
- Increased customer confidence

iv. Choose the Right Platform and Payment Gateway:
Choosing the right platform and payment gateway is extremely crucial for maintaining online payment security. The security of your payment gateway should be your top concern when accepting payments online as you’re handling the sensitive financial data of your customers. You should ascertain that the payment getaway and platform chosen by you is well-known in the industry and has clearly outlined what security measures it uses.

Business can save money by avoiding cyber risks if you spend the initial effort and funds necessary to buy a safe platform and payment gateway. This will help reduce the risk of cybercrime and fraud. The global annual cost of cybercrime is predicted to reach USD 8 trillion in 2023 and it can go up to USD 10.5 trillion by 2025. The key takeaway is that cyber threats can lead to grave consequences and having a secure payment system is the key to ensuring payment security in e-commerce.

v. Updated Operating Systems:

Business must keep their operating systems updated to be certain that your system has the most recent security measures.Keeping your operating systems updated is an important part of reducing the threat of data breaches caused by hackers and fraudsters, as well as minimizing vulnerabilities in the system. The focus should be on being proactive instead of reactive and trying to reduce the chances of cybercrime beforehand.

vi. Payment Tokenization:

Tokenization is a process by which a 16-digit card number gets replaced by a digital identifier known as a ‘token’. This is done for the safety of the original data while allowing payment gateways to securely access the cardholder data and initiate a secure payment.

Fact: Even if a website gets breached and the tokens stored are hacked, it is immensely difficult to reverse-engineer the actual card number from the token itself. To do this, one needs access to the logic used for tokenization, which is not publicly available.

Credit card tokenization helps e-commerce websites improve security, as it eliminates the need for storing credit card data, and reduces security breaches. For more on how tokenization works and impacts online payments, you can read our in-depth blog.

vii. Two-Factor Authentication:

Two-factor authentication (aka 2FA, or two-step verification) is a security method that uses two different methods to authenticate the identity of the user before granting access to a website.Fact: 2FA is not a newly-minted technology, but it has recently become the de-facto method of authentication in the digital age. In 2011, Google announced 2FA for heightening online security for its service. MSN and Yahoo followed suit.When you use NetBanking for a transaction, you are first asked to enter your username and password. As a final confirmation, the bank sends you an OTP on your registered mobile number. This process has been mandated by the RBI and is divided into two levels of authentication:

What the user knows:

In this first step, users fill in their card / NetBanking details such as username and password. This helps the payment gateway recognize which bank the card belongs to.

What the user (and only the user) has:

This step is known as ‘authorization’ and is done via OTP / PIN / CVV. The bank (and the payment gateway) can then confirm that the payment request is initiated by the rightful user.
Two-factor authentication is an extra layer of security added by e-commerce websites to provide a secure payment experience for a customer. It is a customer-facing authentication process, where the transaction is processed only after the user enters a detail that only they could know, or have at hand (like a physical token or a security key). Many banks and e-payment gateways use 2FA for their payment modes.

viii. Verify Transaction Details:

Online financial transactions are risky because they could be completed without actually holding a physical card. Businesses can reduce the risk of unauthorized payments by verifying the details of users, such as CVV, billing address, phone number, and email ID.

ix. Fraud Prevention and Monitoring Systems:
Apart from the mandatory protocols mentioned above, most e-commerce websites and payment gateways have their own fraud and risk prevention systems. Big data analytics and machine learning play a huge role in devising these risk prevention and mitigation systems.

By delving into our customer's data and analyzing patterns, we at Razorpay can discern between a 'normal' and a 'suspicious' transaction with credible accuracy. Apart from this, there is a lot that you as a customer can do to reduce the risk of fraud.

x. Train Employees in Security Measures:
Take steps to make sure that your team understands what is online payment security. Your employees should be able to recognize potential threats and take the appropriate action. Set up seminars and training sessions to thoroughly educate your staff on data protection guidelines, multiple security measures and protocols, and other related topics.

xi.. Explain Security Measures to Customers:
Once the security measures are in place, it is crucial to let your customers know about them so that they feel secure when making transactions on your website. Make an effort to promote the data protection procedures you have put in place.

For instance, inform your clients that two-factor authentication is used by your company to thwart fraudulent online purchases. Mention that your company employs a reliable payment gateway that complies with PCI standards.

Things to Remember Before Making an Online Payment:
Anyone of importance will never ask for your card data/passwords up front. Banks and financial service providers have a safe protocol to gain admin access to an account if the need ever arises.
Passwords are safer when you don't write them down. Keep strong passwords that you can remember, change them frequently, and refrain from writing them down somewhere.
You have the right to dispute suspicious charges on your card or accounts. Raise a chargeback request for any unidentified transaction on your card. You have a legal right to a resolution.

7.9.Ensuring Encryption Effectiveness:

While encryption is a powerful security measure, its effectiveness depends on various factors:

i. **Strong Algorithms:** The encryption algorithms used must be robust and resistant to attacks. Widely recognized algorithms, such as AES (Advanced Encryption Standard), are preferred for their proven security.

ii. **Key Management:** Proper key management is essential for maintaining the integrity of encryption. Keys should be stored securely and rotated regularly to minimize the risk of unauthorized access.

iii. **Regular Auditing:** Regular security audits and penetration testing help identify vulnerabilities and ensure that encryption protocols are correctly implemented.

iv. **User Education:** Educating users about the importance of encryption and secure online practices enhances the overall security posture. Users should be cautious of phishing attempts and practice good password hygiene.

7.10. Conclusion:

Ensuring online payment security has become crucial for running a successful digital business. One little crack in the security system can provide criminals access to client information and enable them to perpetrate financial fraud. The customer might sustain significant financial losses, and your company might experience serious legal repercussions, including fines and a damaged reputation.We are fortunate to have access to cutting-edge security techniques that let you accept consumer payments online securely without endangering your customers' personal information. Follow all possible online payment security methods in your company to provide customers with a safe and reliable experience.Encryption plays a pivotal role in fortifying the security of online payment services. It acts as a powerful shield against cyber threats, safeguarding sensitive financial information and preserving the trust of users. As the landscape of online transactions continues to evolve, encryption will remain a cornerstone of data protection, ensuring that individuals can engage in financial transactions with confidence, knowing that their information is well-protected from prying eyes.

7.11 Keywords:

- Cryptographic
- E-Payment
- Security
- Data
- Customer
- Algorithms
- Secure Transactions
- Cyber Threats
- Encryption etc.

7.12. Self-Assessment Questions:

i. What is cryptographic and explain the importance of cryptography?

ii. What is the purpose and benefits of encryption in E-payments?

iii. Explain some of the key security measures behind digital payment systems?

iv. Explain 11 best practices that business can use to establish a robust mechanism of secure online payment processing?

7.13 References:

i. Adams D. & Bond R. (2000) Secure E-Commerce – A Competitive Weapon, Electronic Commerce Report, UNICOM Seminars Ltd.

ii. Beckett B. (1988) Introduction to Cryptography, Blackwell Scientific Publications, UK. Budge P. (1998) How Safe is the Net? Business Week, June 22.

iii. Cross B. (1999) BT Trust wise – Enabling eCommerce Through Trust. BT Technol J. Vol 17(3), 44-49.

iv. McGuire B. & Roser S. (2000) What Your Business Should Know About Internet Security. Strategic Finance, Vol. 82(5), 50-5

v. Morse S. (1840) US Patent for Morse Code, United States Patent and Trademark Office (USPTO),

Dr. K. Sudheer Kumar

Lesson-8
DIGITAL SIGNATURE AND REMOTE AUTHENTICATION IN E-PAYMENT SYSTEMS

After reading this lesson, you will be able to understand:

Objectives:

- To understand the importance of legal framework for electronic -signatures
- To discuss the properties, advantages and three types of digital signatures
- To describe the application areas of electronic signature and use cases
- To define remote authentication in electronic payments
- To mention Multi-Factor (MFA) Authentication structure

Structure

8.1. Introduction:

A digital signature is used to authenticate digital information — such as form templates, e-mail messages, and documents — by using computer cryptography. Digital signatures help to establish the following assurances: Authenticity The digital signature helps to assure that the signer is who he or she claims to be.Electronic payment system is defined a method of paying for goods or services electronically, instead of using cash or a check, in person or by mail. The electronic payment system has grown progressively over the last few decades as the world advance more on technology development.

History. In 1976, Whitfield Diffie and Martin Hellman first described the notion of a digital signature scheme, although they only conjectured that such schemes existed based on functions that are trapdoor one-way permutations.

The Information Technology Act, 2000 (IT Act), came into effect on October 17, 2000. This legislation provided legal recognition to electronic records and digital signatures, paving the way for their use in various electronic transactions.

8.2. Meaning:

Digital signature—a type of electronic signature—is a mathematical algorithm routinely used to validate the authenticity and integrity of a message (e.g., an email, a credit card transaction, or a digital document.

An example of an electronic signature is when you digitally sign a document by typing your name in a designated signature field. Another example of an electronic signature is a scanned image of your handwritten signature that you insert into a document.A typed name at the end of an email can also be considered an electronic signature.

A digital signature is a type of electronic signature that uses cryptographic techniques to verify the authenticity and integrity of a digital document or message. It involves the use of a public key infrastructure (PKI), which contains a pair of keys: a private key kept by the signer and a corresponding public key made available to others. The signer applies their private key to digitally sign the document, creating a unique digital fingerprint that can be verified using the provided public key. The PKI provides a secure framework for verifying the identity of the signer, preventing tampering with the document, and enabling trust in business transactions.

A digital signature is an electronic, encrypted stamp of authentication on digital information such as messages. The digital signature confirms the integrity of the message.

Remote Digital Signatureis a digital device that differs from the “traditional” ones; in fact, it does not need to be connected to a physical tool. Thanks to RDS, it is not necessary to: bring a dedicated physical device with you; Insert a smart card into a card reader; insert a token into a USB port.

8.3. Understanding the Importance of Legal Framework for Electronic -Signatures:

Electronic signatures are legally binding and enforceable in many countries around the world. In the United States, for example, the Electronic Signatures in Global and National Commerce Act (ESIGN) and the Uniform Electronic Transactions Act (UETA) provide legal frameworks for the use of electronic signatures.

The ESIGN Act is a federal law enacted in 2000 to promote electronic commerce and trust in electronic transactions. The act creates a general presumption (subject to a few exceptions) that electronically signed documents have the same legal validity as hand-signed documents. The UETA is enacted on a state-by-state basis and functions similarly to the federal ESIGN Act.

Other countries also have enacted laws or regulations that recognize electronic signatures. For instance, the European Union (EU) has its Electronic Identification and Trust Services Regulation (eIDAS Regulation). It provides a legal framework for electronic signatures and other electronic identification methods across all member states. In Canada, the Personal Information Protection and Electronic Documents Act (PIPEDA) regulates the use of electronic signatures in certain types of transactions.

Overall, the legal landscape surrounding electronic signatures continues to evolve as more countries and jurisdictions adopt electronic signature laws and regulations. Individuals and organizations need to stay up-to-date with these developments to ensure that their use of electronic signatures remains legally compliant.

8.4. Properties, Advantages and Three Types of Digital Signatures:

i. Digital signatures provide us with three very important properties as under:

a) Authentication,
b) Integrity and
c) Non-Repudiation.

ii. Here are some key advantages of digital signatures in business:

a) Enhanced Security: Digital signatures use cryptographic algorithms to secure documents.

b) Authentication.
c) Cost Efficiency.
d) Time Savings.
e) Global Accessibility
f) Environmental Benefits
g) Efficient Workflow and
h) Legal Validity.

iii. Three different types of electronic signatures:

a) Simple electronic signatures (SES) SES is the easiest type of e-signature to manage, but it's also the one that provides the least validation overall.
b) Advanced electronic signatures (AES).
c) Qualified electronic signatures (QES)

8.5. The Difference Between a Digital and Electronic Signature:

When trying to remember the difference between a digital and electronic signature, it’s similar to how all squares are rectangles but not all rectangles are squares.

Electronic signatures are a broad category, like rectangles. Any signature that isn’t delivered as “wet ink,” or actual ink on physical paper, is an electronic signature.

Digital signatures rely on cryptography to lock the content and ensure that it isn’t changed after signing. They use a certificate generated by a Public Key Infrastructure (PKI). A PKI is a type of encryption that includes:

Public key: Encrypts or “scrambles” data

Private key: Decrypts or “unscrambles” data

The PKI ensures that only the person with the private key can access the document so that the sender can authenticate the recipient’s identity by linking it to the document and maintaining its integrity.

8.6. Three Different Types of Electronic Signatures:

Not all e-signatures have the same level of protection for authenticity, identity, integrity, and authentication. In 2016, the European Union passed the electronic Identification, Authentication, and Trust Services (eIDAS) regulation. This legal framework standardized electronic identification, signing processes, seals and documents across the EU.

The differences between the three types of e-signatures are based on the level of protection they provide.

i. Simple Electronic Signatures (SES):

SES is the easiest type of e-signature to manage, but it’s also the one that provides the least validation overall. An SES is basically just electronic data sent to or associated with other information that someone signs. For example, this could be a PDF that the user downloads, makes a copy of, signs, and sends back via email.

Typically, companies use an SES in cases where they don’t need to verify a person’s identity and believe that the signature is authentic. They’re often used for low-risk documents so the recipient can acknowledge that they read and understood the document.

ii. Advanced Electronic Signatures (AES):

An AES uses a Certificate Authority (CA) to uniquely identify the signatory and validate their identity. Usually, a company uses a delivery service provider that creates audit trails with evidence about the transaction.

A company uses AES when it needs some level of visibility and documentation across authenticity, identity, authentication and integrity.

iii. Qualified Electronic Signatures (QES):

QES is for situations where a company must have documentation across authenticity, identity, authentication, and integrity. It provides the highest level of assurance.

This E-Signature requires:

- Identification using a CA, in-person validation or video
- PKI certificate issued with appropriate technology
- Although it’s the most secure e-signature, QES is also the most difficult verification method.

8.7. Application Areas of Electronic Signature andUse Cases:

For a document to be legally binding, a company often needs to use either AES or QES e-signatures because they are more secure and provide more documentation about the signatory.

i. Contract Management:

By using e-signatures for contracts, companies can digitally transform contract lifecycle management. With e-signatures, companies can send documents in bulk, track signatory completion, and integrate everything directly into a centralized repository.

ii. Purchase Orders:

Many organizations use e-signatures as part of the procurement process. E-signatures enable organizations to ensure that the person has the appropriate signing authority to mitigate fraud risks.

iii. Mortgages:

Banks and lenders use e-signatures as part of the online closing (e-closing) process. As e-closings increased exponentially during the pandemic, companies learned that they save time and money. Using e-signatures for the mortgage closing legal documents is faster, more convenient, reduces errors and provides easier access to documents.

iv.. Claims Processing:

Insurance companies can pay out claims faster using digital processes, making customers happier. However, before making a payment, insurers need to validate the recipient’s identity and get legal documents signed. By using e-signatures, they can digitize the entire claims process and provide better customer service.

v. Licensing Agreements:

Using e-signatures for licensing agreements makes it easier for parties to document the mutual agreement over the use of branded, patented or trademarked intellectual property.

vii. Legal Agreements:

As law firms digitally transform their business models, e-signatures have become fundamental. To enforce documents, firms need to validate and authenticate all signatories. E-signatures give them a way to streamline these processes and mitigate the risk of human error.

viii. Wills, Trusts and Estates:

Trust and estate law has always relied on signed documentation to ensure that a person’s wishes are fulfilled and that trustees meet their fiduciary duties. Usually, when a person wants to make a change to these documents, they need to sign a document in front of a witness to verify their identity. Using e-signatures can streamline these processes, making it easier for attorneys and their clients.

8.8. Method of making an Electronic Signature:

To create an electronic signature, we can use a variety of methods, such as signing with a stylus or finger on a touchscreen device, using a signature pad, or even signing on paper and scanning it to create a digital copy. You can also choose from various software applications and online platforms that allow you to create and insert an electronic signature into documents.

i. Text:In this method, you have the flexibility to personalize your signature by typing your name exactly as you want it to appear. For instance, if your name is Janet Jacob, you can choose to type it as is or customize it according to your preference, such as Janet, J. Jacob, Janet. J, Janet, and more. Additionally, you can enhance the look of your signature by selecting from a range of six pre-formatted text styles that suit the needs of a business.

ii. Draw:Use the Draw style to re-create your signature using:
A mouse or touchpad on a computer. Your finger or stylus on a tab or smartphone.

iii. Upload:With the Upload option, you can use your "handwritten or wet" signature to sign documents. For that, you need to sign on a piece of paper, scan it, or take a photo using a mobile, and save it as a .jpeg or .png file. Next, upload the saved image of your wet signature.Once you choose the preferred signature style, click on the Adopt Signature button, and your e-signature will be automatically placed inside the signature box.

8.9. Different Types of Electronic Signatures:

In the European Union, the law governing the use of electronic signatures is defined by the eIDAS (Electronic Identification, Authentication, and Trust Services) regulation.

As per eIDAS Regulation, there are three types of electronic signatures as under:

i. **Simple Electronic Signature (SES):** This is the most basic type of electronic signature. It can be as simple as typing your name or clicking a button that says "I Agree." It doesn't require any special verification or proof of identity for the signer.

ii. **Advanced Electronic Signature (AES):** An advanced electronic signature is more secure than a simple electronic signature. This type of signature uses a digital certificate to verify the identity of the signer, ensuring that the signature is authentic and cannot be forged.

iii. **Qualified Electronic Signature (QES):** A qualified electronic signature is the most secure type of electronic signature. It is created using a digital certificate issued by a Qualified Trust Service Provider (QTSP). The QTSP is authorized by the government to provide digital certificates and is responsible for verifying the identity of the signature holder.

8.10. Meaning of Authenticate Payment:

Payer authentication requires that your clients present evidence to prove their identity. For instance, they may be asked to provide a username and a password, answer screening questions, or provide a fingerprint or face scan. Sometimes a person can be authenticated through the information provided by the device they are using.

Common categories of authentication are address verification systems, card verification values, challenge-handshake authentication protocols, and 3-D secure (3DS) authentication. Let’s look at each in more detail.

8.11. Types of Electronic Payment Systems:

There are nine types of electronic payment systems as under:

i. Credit and Debit Cards: Widely accepted for online and in-store purchases
ii. Mobile Payment Apps
iii. Digital Wallets.
iv. Bank Transfers and Automated Clearing House (ACH)
v. Online Payment Gateways
vi. Cryptocurrencies.
vii. Peer-to-Peer (P2P) Payment Apps and
viii. Contactless Payment Cards
ix Authentication vs Authorization:

While both payment **authentication and authorization** are important to ensure that a transaction goes through smoothly, the two terms convey different meanings and correspondingly different challenges.

With credit card authentication, the responsibility is on the purchaser to provide adequate proof that they have the right to make the purchase using the method at issue. To do this, the purchaser must offer information to verify that they are the legitimate cardholder and not an impersonator attempting to misappropriate the legitimate card owner's identity to perpetrate an unauthorized transaction.

Payment authorization, on the other hand, is a necessary step that follows the authentication of payment. When you authorize a payment, you take steps to verify that the payment method being used — such as a credit or debit card — is a vehicle that can relay sufficient funds to cover the transaction. The goal of payment authorization is to ensure that the payer has enough money to complete the transaction and that the payment method isn't declined by the payer's bank.

i. Address Verification System (AVS):

The purpose of using an address verification system is to discourage fraud by requiring that the billing address on the card and the one provided by the client are a match. With AVS validation, the client provides a billing address which is then checked for accuracy against the address on file at the bank or credit card company.

AVS puts the payee in control of whether and when to approve a payment, investigate a transaction — something they may decide to do if the address given has only minor discrepancies when compared to the bank's information — or cancel a transaction altogether.

While AVS is easy to implement and doesn't interfere with the purchasing process, a major drawback is the ease with which professional hackers can provide the address associated with a card. Experts in fraudulent AVS (meaning credit card thieves) know all the tricks to locating an address through social media or through an internet search. For this reason, most experts recommend using AVS in conjunction with other independent authentication systems.

ii. Card Verification Value (CVV):

Anyone who uses credit or debit cards is familiar with the CVV numbers on the back of their cards. When a customer attempts to make a purchase without the opportunity to present the physical card — they may when paying for something via a website or over the phone, for example — they'll be asked to provide the three- or four-digit CVV number. This authentication protocol is designed to ensure that the person providing the card number is, in fact, in possession of the card they're using.

The advantage of this type of payment authentication is that it prevents someone who fraudulently co-opted another's credit card number from using the card. Unfortunately, it doesn't stop a credit card thief or another unauthorized user from using a credit card that is in their actual possession. And CVV authentication doesn't prevent an unauthorized user from making note of the CVV number off a card — even if they're not in physical possession of it at the time of the transaction.

iii. Challenge-Handshake Authentication Protocol (CHAP):

The Challenge-Handshake Authentication Protocol is used to thwart bad actors who try to steal a user's payment information by relying on a device-driven authentication system. CHAP periodically re-authenticates the user device during a given online session, using a shared secret as an access point. This cryptographic exchange is referred to as a "handshake." Throughout an electronic exchange, the authorizing party's device sends challenges to the already connected party. This authentication and reauthentication process ensures that the original user is not being interfered with by a third party who has misappropriated the legitimate user's credentials.

CHAP works best in conjunction with other authentication methods that are designed to provide actual payment authentication.

iv.3-D Secure (3DS):

3-D Secure authenticates digital transactions through a mechanism that relays payment and contextual information — such as device identification, billing address, transaction history, purchase amount, and location — to banking institutions to verify a customer's identity. The user verifies their identity through email, text, or phone.

3DS is a risk-based payment authentication method that handles transactions differently based on the level of risk associated with the payment. Using 3DS technology is considered a best practice for authenticating transactions as it uses multiple data points for identity verification.

8.12. Remote Authenticationin Electronic Payments: In remote electronic payments, frauds occurs when a person who is not the legitimate owner of an identity or financial account either fraudulently creates a new account or takes over an existing digital account for the sole purpose of committing an illegal activity using stolen payment credentials or unauthorized payment.information.

Authentication of the customer and payment method should take place at each step in the remote payment process – account creation, enrollment and transaction – to identify, prevent and mitigate fraud attacks. Authentication fraud can occur when fraudsters take advantage of legitimate owners who conduct a digital financial activity, such as through a mobile phone app, mobile browser or PC internet browser, to:

- Open a bank account or credit card through mobile or online banking
- Enroll a bank account or credit card with a third-party payment provider/digital wallet
- Pay for a purchase
- Transfer funds

In all cases, the fraudulent customer is not present physically at the financial institution or merchant point of sale.

8.13. Methods of Remote Authentication:

This section describes several methods and types of data collected to verify and authenticate an individual during remote enrollment and transaction processes. Verifying identity and providing strong authentication are key steps to preventing the occurrence of fraud at the very beginning of the customer account relationship. Stakeholders need to have a good understanding of the different approaches and tools available to be able to apply the appropriate methods depending on the payment method, customer information, transaction type and risk level.

Identity (ID) proofing occurs when an individual opens a bank or credit card account, signs up for a new banking service or adds a biometric method to the account for future authentication. This process verifies the individual's connection to his or her real-world identity to assure the individual is who he or she claims to be. Once a customer has a proven identity, the veracity of information provided to confirm the user ID is accepted. Authentication covers multiple steps, including enrollment with PSPs and online merchants, funds transfers and account recovery. Authentication can be explicit (e.g., requiring the individual to enter a passcode or perform a biometric check) or implicit (analyzing context, transaction, and device information to detect unusual behavior that could indicate fraud).

More specifically, authentication is as under:

- Corroborates a claimed identity
- Validates that an entity is a real person, not a machine or bot12
- Affirms that an individual is not likely a fraudster
- Authorizes a specific financial request

Description of current authentication methods While there are many authentication methods to prevent remote fraud, these methods provide different levels of protection and may function independently of each other. Because of the changing nature of fraud, the effectiveness of some methods is declining. These methods are being replaced with stronger, but not widely adopted, alternatives across the payments industry. The sophisticated attacks to the payment system expose flaws in current authentication practices and create a need to develop more complex defense strategies. Multi-layered and multi-factor authentication (MFA)13 are considered best practices for stronger authentication in the industry. If applied appropriately as a first step, these methods can help prevent authentication fraud from occurring later in the payment process. Multi-layered authentication Multi-layered approaches combine several authentication methods to confirm the identity of the account holder during onboarding, enrollment and when conducting a payment transaction. Layers can include passive14 authentication data (e.g., mobile device intelligence, device binding, one-time passcodes or OTPs, license scanning), as well as username and password, knowledge-based authentication (KBA), biometrics, machine learning and behavioral analytics. While not prescriptive on which options to use, layering implies implementing at least two authentication methods, known as the waterfall process for identity proofing.15 Layering enables the provider to use the appropriate authentication methods based on transaction value, type of mobile device and type of payment (new or recurring).

8.14. Multi-Factor Authentication (MFA):

Applying MFA to confirm the customer’s identity when he or she logs into a remote banking or payment app makes it more difficult for an unauthorized person to locate the device, network or database and access the remote app. MFA takes layering a step further by requiring use of one authentication method from each of three distinct factors: something you know, something you have and something you are. Individually, any one method or factor may not provide enough protection from fraudsters. However, if one factor is compromised by a fraudster, having a second factor adds more protection to prevent fraudsters from obtaining enough information to authenticate and access an account. For example, if a fraudster enters a legitimate password, he also will need the registered device and biometric to make a fraudulent remote transaction.

i. Benefits of Multi-Factor Authentication(MFA)

a. Provides a higher level of security than single-factor or two-factor authentication.
b. Provides some consistency with authentication approaches.

ii. Challenges of Multi-Factor Authentication (MFA):

a. MFA can increase customer friction when indiscriminately applied to all use cases and circumstances. If there are too many authenticators or they are too complicated, customers will abandon their online shopping carts. As a result, customers may choose easier, albeit riskier, MFA options (such as PIN or password) over stronger options, such as biometrics.

b. Consumers are accustomed to using passwords, which are likely to remain the default first MFA factor for the near future. Forrester reports that 70% of organizations still rely on password-centric authentication.

c. While more providers are implementing MFA, anecdotal evidence suggests its use is inconsistent:

- Lack of standardization and minimal data to measure the effectiveness of MFA complicate how to determine which vendor solution is most effective for a particular use case. As a result, many organizations are taking a "wait-and-see" approach or have implemented MFA only for their highest-risk portfolios.

- The rate of change at which fraudsters are able to invent new fraud attacks has made some organizations wary of making incremental improvements. They may defer upgrades until the "next best system" has been identified.

d. FFIEC guidance on multi-layered authentication focuses on FIs, although it encourages non-banks to consider MFA's value. However, it remains a gap that may put the broader payment system and consumers at risk, since payment instructions flow between, and therefore impact, FIs, processors, networks and merchants if all parties in the process do not apply effective authentication controls.

8.15. Data Collected to Support Remote Authentication:

Data collection refers to the process of gathering data about the individual enrolling in a payment service or initiating a financial (banking or payment) transaction, the device used to conduct the transaction, and the type of transaction. Data collected for verification or authentication purposes comprise the attributes (identity, device, or knowledge) that describe an individual. Examples include name, email, fingerprint, swipe angle, apps loaded and internet protocol (IP) address. Some data is mandatory, while collecting other data may depend on the need or type of transaction, or as a best practice. Organizations collect data elements from a variety of sources, initially when account ownership is established. The data strengthen over time through the above-mentioned techniques to provide a high degree of trust at account login and during a transaction.

i) Mandatory Data:

Financial institutions are required under Know Your Customer (KYC) and Customer Identification Program (CIP) regulations to collect, verify, and record a minimum set of data elements that provide evidence of a customer's identity at account opening or onboarding. Required data elements include name, date of birth, address, identification number (e.g., Social Security number) and documented evidence of identity and address.

ii) Typically Required Data:

FIs also collect digital and mobile identifiers, such as email address, phone number, preferred or registered device.

ii) User-Generated Authentication Data:

Once the FI approves an application, the user is required to establish a username and password to access the account and then, to set up multiple security questions and answers, which account holders later use to re-verify account ownership or reset passwords.

iv) Optional Data:

Advanced account opening processes that extend beyond standard KYC may ask for additional information to further identify and subsequently, authenticate the customer. Examples of optional data include PINs and biometrics (facial, fingerprint and voice recognition, selfies and video). For remote account openings, organizations may request biometrics to establish a link between the ID document holder and the ID document, or to establish that the applicant is a live person and not a bot – automated software that runs per instructions without human intervention. Common techniques include CAPTCHA (distorted letters and numbers), and reCAPTCHA (i.e., a grid containing multiple photos where the customer selects grid boxes displaying a particular object).

v) Invisible Authentication:

Data organizations also can collect data about the behavior of the legitimate owner and his or her device through behavioral biometrics, behavioral analytics, advanced algorithms and device identification.

These techniques are as under:

- Predict which transactions are normal or anomalous (e.g., type, size, frequency, location).

- Analyze biometric behavior typical to the account holder (e.g., typing speed, swipe direction, angle of handheld device) to detect automated bot or imposter attacks.

- Examine all aspects of a device (operating system, IP address, geolocation, browser history and jailbreak status) to establish genuine ownership. Machine-generated authentication data When organizations detect an elevated level of risk or one that exceeds a certain threshold during login or when initiating a transaction, they communicate with the account holder to verify his or her identity. This is typically done by sending a code via SMS or email to the account holder’s device, which the customer then keys into a field on the mobile or website.

8.16.Conclusion: Instead of reaching for cash or writing cheques, we can now effortlessly transfer funds electronically with just a few clicks or taps. Besides, electronic payment systems have revolutionized the way we handle our finances, making transactions quicker, more efficient, and accessible to anyone with a bank account.The success of digital payments in India has been remarkable, driven by the government's push towards a cashless economy and the adoption of UPI. Digital payments have had a positive impact on the economy, leading to financial inclusion, reducing the use of cash, and boosting the fintech industry.Research findings suggest that the use of mobile devices for making online payments is increasingly becoming popular due to a large user base of mobile phones. This payment method best suits micropayments and offers more convenient and secure payment transactions if appropriately implemented.

8.17 Keywords:

Data
Digital Signature
Electronic Signature
Digital Payment
Remote Authentication
E-Payment
Security

Multi-Factor Authentication (MFA) etc.,

8.18. Self-Assessment Questions:

i) What is digital signature and electronic signature? and explain the differences between them?
ii) What is remote authentication in in e-payments?
iii) Explain various types of electronic payment systems?
iv) Mention different types of electronic signatures?
v) Explain various methods of remote authentication?

8.19. References:

1. 1] Ferguson, Niels, Bruce Schneier, and Tadayoshi Kohno. Cryptography engineering: design principles
and practical applications. John Wiley & Sons, 2011.
[2] Agnew, Gordon. "Secure electronic transactions: overview, capabilities, and current status." Payment
technologies for E-commerce.Springer Berlin Heidelberg, 2003.211-226

1] Ferguson, Niels, Bruce Schneier, and Tadayoshi Kohno. Cryptography engineering: design principles
and practical applications. John Wiley & Sons, 2011.
[2] Agnew, Gordon. "Secure electronic transactions: overview, capabilities, and current status." Payment
technologies for E-commerce.Springer Berlin Heidelberg, 2003.211-226
1] Ferguson, Niels, Bruce Schneier, and Tadayoshi Kohno. Cryptography engineering: design principles
and practical applications. John Wiley & Sons, 2011.
[2] Agnew, Gordon. "Secure electronic transactions: overview, capabilities, and current status." Payment
technologies for E-commerce.Springer Berlin Heidelberg, 2003.211-226

1. Miva. The History of Ecommerce: How Did It All Begin? —Miva Blog. Available online: https://www.miva.com/blog/the-history-of-ecommerce-how-did-it-all-begin/ (accessed on 16 June 2020).

2. Alam, S.S.; Ali, M.H.; Omar, N.A.; Hussain, W.M.H.W. Customer satisfaction in online shopping in growing markets: An empirical study. *Int. J. Asian Bus. Inf. Manag.* **2020**, *11*, 78–91.

3. Noor Ardiansah, M.; Chariri, A.; Rahardja, S.; Udin, U. The effect of electronic payments security on e-commerce consumer perception: An extended model of technology acceptance. *Manag. Sci. Lett.* **2020**, *10*, 1473–1480.

4. Soare, C.A. Internet Banking Two-Factor Authentication using Smartphones. *J. Mob. Embed. Distrib. Syst.* **2012**, *4*, 12–18.

5. Kaur, J.; Singh, H. E-Banking Adoption: A Study of Privacy and Trust. *Int. J. Technol. Comput.* **2017**, *3*, 314–318. [**Google Scholar**].

Dr. K. Sudheer Kumar

Lesson-9

MOBILE PAYMENTS AND DIGITAL WALLETS OVERVIEW

After reading this lesson, you will be able to understand:

Objectives:

- To understand mobile payment: proximity and remote
- To mention the importance of mobile payment
- To define the functions of mobile money, electronic money and mobile banking
- To describe benefits of Mobile Payments
- To define Mobile payment technology: Digital wallets and rising payment applications
- To mention Multi-Factor (MFA) Authentication structure

Structure

9.1. Introduction:

A payment system is a set of instruments, bank procedures and, usually, interbank fund transfer systems that guarantee the circulation of money. Payment systems are traditionally classified as either high value or low value. Many banks have recently adopted technology into their banking apps that allow customers to send money instantly to friends and family members directly from their bank accounts. Mobile payments are also made on site at stores by scanning a barcode on an app on your phone, accepting payments from convenience stores to large, multi-national retailers.

The cost of the purchase may be deducted from a pre-loaded value on the account associated with the particular store, or paid by credit or debit card. Payment information is encrypted during transmission, so it is thought of as being a safer payment method than paying with a debit or credit card.

Mobile payments first became popular in Asia and Europe before becoming more common in the United States and Canada. Early on, mobile payments were sent by text message. Later, technology allowed for pictures of checks to be taken via cell phone camera and sent to the payment recipient. This technology eventually morphed into mobile check deposit capabilities for banking apps.

Since 2014, apps such as PayPaland Apple Pay were developed that allow payment by passing a smartphone screen displaying a special barcode under a store's barcode scanner.

They also allow the user to simply tap their phone against a contactless credit card terminal, paying instantaneously.

A mobile payment is a money payment made for a product or service through a portable electronic device such as a tablet or cell phone. Mobile payment technology can also be used to send money to friends or family members, such as with the applications Google Pay, PhonePay, PayTM, PayPal etc.,

9.2. Meaning:

A mobile payment is the transfer or payment of funds typically to a person, merchant or business for bills, goods and services, using a mobile device to execute and confirm the payment. The payment tool can be a digital (virtual or e-) wallet, mobile browser, or SIM toolkit / mobile menu.

Mobile payment is one of the many mobile financial services (MFS) available today and is seen as a gateway to other mobile financial services such as, mobile banking, insurance, credit/lending and investment products. More recently consumers are adopting cryptocurrency for payments, trading, savings and investing.

A mobile payment can be person to person (P2P) or consumer to consumer (C2C) transaction as well as consumer to business (C2B), business to consumer (B2C) or business to business (B2B) transaction. A P2P payment can be referred to as a mobile money transfer (MMT) while more commercial C2B, B2C and B2B transactions could be more strictly defined as mobile payments.

9.3. Forms of mobile payment: proximity and remote:

Mobile payments can be classified as proximity or remote payments in that they occur within a proximity location (distance and range) such as a point of sale (POS) or remotely when paying a bill online, sending money to someone (e.g. to split a bill) or when sending a remittance.

With proximity payments the customer’s mobile phone and the merchant’s physical POS or mobile POS are in the same location. The merchant POS location may be attended (in-store) or unattended (self-check-out, vending machine, unmanned store). Both parties communicate and transact using a proximity mobile payment technology such as near field communication (NFC) wallet, QR barcode or Bluetooth low energy (BLE). Announced in 2021, Samsung smartphones will no longer feature magnetic strip technology (MST) with its Samsung Pay wallet as Mastercard, a major card issuer is planning to remove magnetic strips from cards starting in 2024 as the more secure EMV (Europay, Mastercard, Visa) chip and pin cards become standard.

Remote payments are made over a fixed or mobile (internet) telecommunication network irrespective of the customer’s location. Remote payments can support bill payments and merchants that don’t have physical POS such as a street vendor but also online merchants that don’t have a physical presence or sell digital products and services.

i.Types of Digital Wallets:

There are several types of digital wallets in India designed for users based on their requirements and usage as follows:

a) **Closed Wallet:** A specific company or service provider offers this wallet and, can only be used for transactions within the provider's ecosystem.

b) **Semi-Closed Wallet:** They are used for a broader range of transactions with fewer withdrawal limitations to a bank account. They have both online and offline purchases.

c) **Open Wallet:** Open wallets have flexible coverage. They allow users to store funds and make payments across a wide range of merchants and service providers and can be linked to multiple sources, such as payment cards and bank accounts.

9.4. Functions of mobile money, electronic money and mobile banking:

Mobile money or m-money as defined by the IMF "is a pay-as-you-go digital medium of exchange and store of value using mobile money accounts which is typically offered by a mobile network operator (MNO) or another entity in partnership with an MNO and often independent of a traditional banking network". A bank account is not necessary to use mobile money services as customers can use a basic mobile phone and register with a mobile money agent. The mobile money agent offers a virtual account / mobile wallet linked to the customer's mobile phone number and allows customers to perform transactions with minimal physical contact using a mobile money menu system such as the SIM toolkit with SMS notification delivery, USSD or through a mobile App.

Mobile money has high levels of market penetration in many low- and middle-income economies, particularly among the unbanked and underbanked populations. The mobile money entity is serviced by a large agent network and exceeds the distribution and reach of the traditional branch banking network in that market. According to the GSMA there were 310 live mobile money services in 96 countries as of 2021.

Electronic money or e-money is a digital alternative to (fiat) cash (essentially pre-paid money) stored electronically on cards, devices or online systems which can be used to make cashless payments to individuals and businesses. Examples of e-money included funds stored in a mobile money account, a prepay card or an online account like Paypal or Revolut. Safaricom's M-PESA, Orange Money, MTN Mobile Money (MoMo) are just some examples of mobile money and e-money solutions. Safaricom's M-PESA in Kenya alone serves over 30 million customers and in 2021 it was announced that half of Kenya's GDP is now transacted on the M-PESA platform.

Mobile banking services on the other hand are linked to a formal bank account with customers using their official bank's mobile application on their smartphone, mobile browser or a linked (credit/debit card) digital wallet on their phone to access it banking services.

Telecom operators such as Orange are also investing in banking services launching Orange Bank in France 2017 and later expanding into Spain. The operator faces intense competition in Europe but could succeed if the group is prepared to make a sustained investment in turning Orange into a financial services brand.

NTT DoCoMo is another example of a telecom operator establishing itself as a player in financial services. Finance and payment services such as d Payment and d Card have been one of the main drivers behind the success of NTT Docomo's Smart Life business which also includes content/lifestyle solutions.

Payment service allows people to pay for purchases made on online shopping sites or physical retail stores through their monthly telephone bill (carrier billing). The primary source of revenue for d Payment is the commission payable by the merchants to Docomo.
d CARD is a credit card that can be used for payments both at merchants supporting Docomo's own brand "iD", as well as the international brands (Visa and Mastercard) chosen by customers when they join the credit card service. d Card generates revenue from the card issuer's share of the commissions paid by the credit card merchants, interest in credit instalment payment services and the annual membership fee.

9.5. Importance of mobile payment:

Thanks to the revolution of digital wallets in online payments, most of the transaction processes have been made easy and hassle-free. Digital Wallets in India have become a great help in the financial part, as one can avoid manually entering the details during payments or visiting the bank to make payments. Digital wallets made it easier and more accessible to all, where one could make instant payments simultaneously.

Digital wallets in India offer robust security measures to protect users' sensitive information and transaction details. Thus, making it an essential online payment mode, digital payment has been the preferred choice for users and business owners.Mobile payment technology offers quick payment processing options. There is no need for data entry, and it reduces wait times. Customers also receive the option to choose digital receipts or invoices.Mobile payments are a popular way to accept in-person customer payments thanks to their security, speed, and level of convenience.

With mobile payments, you can accept card and mobile wallet payments from virtually any location as long as you have a mobile POS, smartphone, or other mobile device configured with a credit card payment app to collect scan to pay or tap to pay NFC mobile payments.

Then shoppers can use an EMV chip card or mobile wallets like Google Pay or Apple Pay (that have contactless NFC technology) to pay in-store or at a restaurant without having to present their credit card.

Mobile payment statistics and trends:

The usage of mobile payments is increasing rapidly. In fact, studies show that:

i. According to one survey in Spain, of the 34% of respondents who currently pay with their mobile device, almost seven out of 10 (67%) say they have increased their use since the beginning of the pandemic.

ii. It's estimated that there will be 1.31 billion mobile payment transaction users worldwide in 2023, up from 950 million users in 2019.

iii. By 2024, the global mobile payment market size is estimated to be 3 trillion USD.

iv. 70% of millennials around the globe enjoy discounts and reward offers as incentives for using mobile payment methods.

v. 46% of consumers globally say they believe using contactless payment methods like mobile wallets is one of the most important safety measures for stores to follow.

vi. Mobile purchases are also gaining popularity online — according to our recent payment trends report, 60.2% of online purchases from April to August 2022 were mobile.

9.6. Mobile payment systems in India:

Some of the mobile payment systems in India are: Paytm, Freecharge, Mobikwik, Oxigen, MRupee, Airtel Money, Jio Money, SBI Buddy, itz Cash, Citrus Pay, Vodafone M-Pesa, Axis Bank Lime, ICICI Pockets, SpeedPay etc.

Modes of Digital Payments:

i. Unified Payments Interface (UPI):

Unified Payments Interface (UPI) is a system that powers multiple bank accounts into a single mobile application, merging several banking features, seamless fund routing & merchant payments into one hood. It also caters to the "Peer to Peer" (P2P) collect request which can be scheduled and paid as per requirement and convenience.

ii. Bharat Interface for Money (BHIM):

Bharat Interface for Money (BHIM) is a mobile app for easy and quick payment transactions using Unified Payments Interface (UPI). User can make instant bank-to-bank payments and pay and collect money using Mobile number, Bank a/c and IFSC code, Aadhaar number or Virtual Payment Address (VPA).

BHIM has the facility to scan & pay through QR code. User can check transaction history and can also raise complaint for the declined transactions by clicking on Report issue in transactions.

BHIM is available in 20 regional languages (English, Hindi, Marathi, Tamil, Telugu, Malayalam, Oriya, Punjabi, Gujarati, Marwari, Haryanvi, Bhojpuri, Urdu, Konkani, Manipuri, Mizo, Khasi, Kannada, Bengali, Assamese) for better user experience.

Users can also make transaction using from their feature phone as well by dialing *99#.

iii. UPI 123PAY:

UPI 123PAY is an instant payment system for feature phone users who can use Unified Payments Interface (UPI) payment service in a safe and secure manner. Feature phone users will now be able to undertake a host of transactions based on four technology alternatives. They include calling an IVR (interactive voice response) number, app functionality in feature phones, missed call-based approach and proximity sound-based payments.

iv. UPI Lite:

"UPI LITE" offers a wallet in BHIM-UPI app for an amount of up to ₹2,000 on a smart phone, eliminating the need for the user to first obtain electronic authorization from his/her bank while making the payment, offering the user better experience in terms of improved speed and transaction success rate.

v. Cards (including RuPay Debit Cards):

Debit Cards, one of the many payment modes, are issued by banks that allow individuals to purchase items at physical stores through Point of Sale (POS) devices or e-commerce marketplaces. RuPay Debit Cards, developed by National Payments Corporation of India

(NPCI) was launched by the Government of India to allow individuals to make payments digitally. To get a RuPay debit card, you can reach out to your bank and ask them to issue you one.

vii. Immediate Payment Services (IMPS):

Immediate Payment Services (IMPS) is a real-time interbank electronic fund transfer service capable of processing person to person (P2P), person to account (P2A) and person to merchant (P2M) transactions. Individuals can make payments 24x7 using their mobile number, Aadhaar number, bank account and IFSC code. Users can access IMPS through multiple channels such as mobile, internet, ATM and SMS.

viii. Aadhaar Enabled Payment System (AePS):

Aadhaar Enabled Payment System (AePS) is a bank led model which allows online interoperable financial inclusion transaction at Point of sale (MicroATM) through the Business correspondent of any bank using the Aadhaar authentication. AePS allows you to do six types of transactions, the inputs required for a customer to do a transaction Bank Name, Aadhaar Number, Fingerprint captured during enrolment.

Banking Services Offered by AePS:

- Cash Deposit
- Cash Withdrawal
- Balance Enquiry
- Mini Statement
- Aadhaar to Aadhaar Fund Transfer
- Authentication
- BHIM Aadhaar Pay

ix. BHIM Aadhaar Pay enables Merchants to receive digital payments from customers over the counter through Aadhaar Authentication. It allows for any Merchant associated with any acquiring bank live on BHIM Aadhaar Pay, to accept payment from customer of any bank by authenticating customer’s biometrics.To be able to affect the same, merchant should have an Android mobile with BHIM Aadhaar app and certified biometric scanner attached with mobile phone/Kiosk/Tablet on USB Port or Micro-ATM/POS, mPOS. Both Customer and Merchant should have their Aadhaar linked to their Bank Account.

x. Bharat Bill Payment System (BBPS):

Bharat Bill Payment System (BBPS) is a one-stop platform that provides an interoperable and easily accessible recurring and bill payment service to consumers via multiple channels like Internet Banking, Mobile Banking, Mobile Apps, UPI, etc. Users are able to bill payments across various categories including electricity, gas, water bills, telecom, DTH, etc.

xi. National Electronic Toll Collection (NETC) FASTag:

NETC FASTag provides an easy and convenient digital payment mechanism for toll payments. This is an interoperable solution available to individuals nationwide. With the use of Radio Frequency Identification (RFID) technology, the FASTag device allows for making toll payments directly while the individuals vehicle is in motion.

xii. E-RUPI:

E-RUPI is a person and purpose specific, contactless and cashless digital payment solution. It can be issued as a prepaid QR code or SMS based electronic voucher which can be used by the Government/Private organizations for delivery of a specific subsidy or welfare benefit to the targeted citizens. The beneficiaries will be able to redeem e-RUPI voucher without a card, digital payments app or internet banking access, at the merchants accepting e-RUPI, simply by showing SMS or QR code. This contactless e-RUPI is easy, safe, and secure as it keeps the details of the beneficiaries completely confidential. The entire transaction process through this voucher is relatively faster and at the same time reliable, as the required amount is already stored in the voucher.

xiii. Unstructured Supplementary Service Data (USSD) / *99#:

*99# is a USSD based digital payment and banking service. Customers can avail this service by dialing *99#, a “Common number across all Telecom Service Providers (TSPs)” on their mobile phone and transact through an interactive menu displayed on the mobile screen. *99# service is currently offered by almost all leading banks & all GSM service providers and can be accessed in 13 different languages including Hindi & English.

Key services offered under *99# service include:

- Interbank account to account fund transfer
- Balance enquiry
- Mini statement besides host of other services

9.7. Benefits of Mobile Payments:

The most obvious benefit of mobile payments is the elimination of a physical wallet. Not reaching and pulling out cash not only saves time but is safer as well as nobody is able to see the contents of your wallet or purse.

Touch ID in the form of a fingerprint scan or PIN input makes mobile payments more secure than a physical credit card. Since individual security codes are generated by the mobile service for each transaction, this method of payment is significantly safer than using a physical card. Merchants will usually not check identification, so accepting mobile payments is a smart move for them as well, as they will not have to deal with fraudulent activity as much.

An additional benefitthough a minor one for most peopleis that when you are with other people, they are not able to tell what card you have. Users with low credit scores and credit cards with low limits and high APRs might not want, say, an interviewer or date to know these things, and mobile payments offer an additional level of personal privacy.

Sixteen benefits of mobile payments:

There are numerous benefits that lend themselves to the global widespread adoption of mobile payments.

i. Reduce expenses:

Opting for mobile payments can help you reduce expenses in a few ways. You don’t need to buy expensive point of sale (POS) equipment or paper and ink due to the ability to email receipts. And because you can use a tablet or smartphone as your mobile point of sale terminal, the only external cost you’ll need to set it up is a card reader.The cloud-based subscription models that mPOS systems have also generally mean low sign up and monthly maintenance expenses.

ii. Improve cash flow:

When using mobile payments, customer funds are transferred to your account either instantly or within a few days. This means you get money faster and, because customers can pay as long as they have their personal mobile device on hand, you’re more likely to receive payments from customers who prefer paying with their mobile wallets.

And considering over one-third of mobile wallet users now have three or more mobile wallets like Google Pay and Apple Pay installed on their smartphones, accepting these alternative payment methods is crucial in today's retail landscape.

In short, with mobile payments, you increase your chances of getting more money from more customers faster than you would with traditional payment methods.

iii. Easily integrate loyalty programs:

Since customer information is stored in mobile payment apps, coupons or discounts can quickly and easily be sent out to specific customers to reward repeat purchases.

These loyalty programs can include:

- **Points loyalty programs:** Customers get points for each transaction and can put them toward discounts or free products.
- **Tiered loyalty programs:** A certain amount of purchases unlocks a new tier of reward points or discounts once the specified number of purchases has been made.
- **Hybrid loyalty programs:** Combine two types of loyalty programs for greater incentives.

iv. Get insights into actionable data:

Using a mobile point of sale system means you have instant and secure access to key customer data.This data can help inform you of your current customers' purchasing behavior and give you the opportunity to further tailor your products, services, or overall customer journey funnel.Data types include how frequently customers shop at your business, their average spend, preferred payment methods, and the products they buy the most.

v. Increase customer convenience:

By adopting mobile payments for your business, customers can leave their wallets at home and still complete purchases.Alongside this, adding a minimum of one mPOS to your store can improve the customer experience by making it faster and more flexible. And depending on the mobile POS system, you'll be able to accept the most popular (and customer-preferred) payment options anywhere in your store or on the go. Accepting a wide range of payment options will help you reach more people and see an uptick in customer loyalty long-term.

vi.. Keep competitive with more ways to pay:

How likely a personfrequents a business if a customer can't pay with a firm's go-to payment method?

By offering multiple ways for customers to pay via mobile payments, customers are staying ahead of the competition.

When investing in an mPOS system, choose one that can process the following types of frictionless payments:

- Contactless (or EMV chip) credit cards
- Digital wallets like Apple Pay, Google Pay, and Click to Pay
- QR code payments

vii. Better payment security:

Mobile payment apps use an encrypted or protected code to shield customers' personal data. This means that customers' real card numbers are never stored on either their personal device or your mobile payment equipment or software.

Because of this, payment security is increased and your liability is significantly lower.

viii. Simplify bookkeeping:

Alongside actionable customer data, using an mPOS system also works to collect the following kinds of information for your business:

- Sales information
- Payment records
- Inventory updates

All of these benefits act as a bonus to mobile payments main upside, which is improving the customer experience and making it easier to accept payments on the go.

ix.Uses of Digital Wallet: Digital wallets in India can be used for various types of transactions, making the whole digital payment process smooth and hassle-free:

x. Online Shopping: Digital wallets simplify the checkout process for e-commerce websites and mobile apps.

xi. Bill Payments: Digital wallets make it easier for users to make recurring payments directly and instantly for utility bills, mobile recharge and other charges.

xii. Ticket Booking: This can be used to book flights, trains, buses, and movie tickets online instantly by avoiding long waits in queues and buffering or network issues (done till here)

xiii. Food Delivery and Dining: Payments have been made easy, and one can avoid waiting in long queues as most dining and delivery apps now accept payments via digital wallets.

xiv. Transfers to Other Individuals: As digital wallets are easily accessible to many, users can send money to friends and family instantly through digital wallets.

xv. In-Store Payments: Since the increase in online payments, physical retailers now accept digital wallet payments.

xvi. Travel Expenses: Using digital wallets is handy for paying travel expenses such as hotels, taxis, and other costs.

9.8. Mobile payment technology: Digital wallets and rising payment applications:

A digital wallet is an application on the smartphone which stores banking credit/debit card as well as loyalty cards and coupon information. Near field communication (NFC) is the most dominant technology linking debit/credit cards to the wallet enabling contactless payments at the POS. Wallets also offer payment via QR code where customers scan the QR code at the merchant's POS. Operator wallet apps such as Turkcell's Paycell and Vodacom's VodaPay also offer QR payment functionality for their merchant network – where customers pay through funds held on the (mobile) wallet or through a linked banking credit/debit card. QR code has become a popular payment feature across many super apps. In the case of the VodaPay super app, customers can also make payments/partial payments using coupons and cashback rewards.

E-Wallets are defined by Worldpay, a global payments processor as "an electronic card used for transactions made online through a computer or a smartphone, like a credit card or debit card. When used with a smartphone, consumers store the credentials of their preferred card for payments and use biometrics to authorize the transaction." Worldpay cites Alipay, WeChat Pay (both strong in China), PayPal (global), Qiwi and Yandex Money (both strong in Russia) as examples of such eWallets. But Apple Pay, Google Pay and Samsung Pay are also a form of E-Wallet, albeit one that is explicitly linked to a mobile device. With the rapid growth of online shopping, usage of all these wallets is rising steadily. See Cashing in on the end of cash.

According to Worldpay, Digital wallets accounted for 48.6% of global e-commerce transaction value 2021 equating to just over US$2.6 trillion. Worldpay projects wallets will rise to 52.5% of transaction value in 2025. Worldpay estimates that by 2025, e-commerce is expected to account for 12% of global consumer spend, with 59% of that e-commerce spend transacted via mobile devices.

Global POS payment methods via digital wallet is expected to rise from 29% of transaction value in 2021 to 39% by 2025 with POS cash payment forecasted to decline from 18% of transaction value in 2021 to 10% by 2025.

According to Worldpay, this growth in digital wallets will be driven by innovation such as improvements to the check-out experience offering advanced credit solutions such as buy now pay later (BNPL) and faster real-time payment infrastructure. BNPL represented 2.9% of global e-commerce transaction value in 2021 and Worldpay expects this to rise to 5.3% of e-commerce by 2025. BNPL players include Klarna, Afterpay (acquired by Square) and PayPal. Worldpay points to the "anchor role" digital wallets are increasingly playing in e-commerce marketplace ecosystems as local wallets transform into regional and global super apps" and points to wide acceptance and usage of digital wallets in Asia Pacific and in particular, the popularity of super apps such as Alipay and WeChat Pay. The digital wallet's share of e-commerce transaction in Asia Pacific is projected to rise from 68.5% in 2021 to 72.4% (over US$3.1 trillion) in 2025.

A super app offers a range of e-commerce (lifestyle) services under one app facilitating payment transactions between users and merchants on the platform and offering a range of financial services beyond payment such as credit, savings, and investment. See Can VodaPay transfer Alipay to South Africa? While WeChat evolved out of a messaging service in China, and Grab evolved out of a taxi booking service in Malaysia, many of today's popular super apps have developed out of mobile payment services such as Alipay in China, Paytm and PhonePe in India. The addition of payments and financial services has helped to unlock the success of other such as Wechat, GrabPay, Gojek's GoPay in Indonesia.

9.9. Future of digital wallets:

Future trends in mobile wallets are the enhancement of loyalty rewards, security and simplicity, artificial intelligence, and cryptocurrency. Also, companies that have investments in mobile wallets have been devising ways to expand their reach in rural areas, which can significantly impact the country's development. The government also has encouraged private and public partnerships to increase the volume of transactions through mobile wallets.

In May this year, the Reserve Bank of India has issued a guideline for all PPIs, including digital wallets, to become interoperable by April 2022. This regulation removed the limitation of using the amount in one wallet only on expenses made through the same wallet. Users can send money from one mobile wallet to various other wallet brands and withdraw cash from Point-of-Sale machines. This move will lead to increased acceptance and volumes for wallet providers. More importantly, this interoperability can expand digital adoption and payments as it will provide more value and ease of use for current and new customers.

Other digital payment modalities have also disrupted the financial payments landscape in India, with the Unified Payments Interface (UPI) being the largest one, perhaps. In Quarter 1 of 2021, around 1.13 billion transactions were made through mobile wallets, while UPI-based payments numbered around 2.3 billion. The value of the transactions was about INR 411.75 billion for mobile wallets and crossed INR 5 trillion for UPI. Stay tuned to this space to read more about UPI in India in our upcoming blog post!

9.10. Conclusion:

In conclusion, digital wallets provide a number of benefits to consumers and merchants alike. From increased convenience to enhanced security, digital wallets offer a compelling value proposition for the market. Digital wallets are becoming an increasingly popular payment option for consumers. They offer convenience, security, and speed, making them a desirable alternative to traditional payment methods.The success of digital payments in India has been remarkable, driven by the government's push towards a cashless economy and the adoption of UPI. Digital payments have had a positive impact on the economy, leading to financial inclusion, reducing the use of cash, and boosting the fintech industry.

9.11. Keywords:

- Mobile Payments
- Digital Wallets
- mobile money,
- electronic money
- mobile banking
- payment applications
- BHIM Aadhaar Pay etc.,

9.12. Self-Assessment Questions:

i) Explain mobile payments and importance of mobile payments?
ii) Define the functions of mobile money, electronic money and mobile banking?
iii) Explain various modes of digital payments?
iv) Explain various benefits of Mobile Payments?
v) Bring out the scenario of mobile payment systems in India?

9.13 References:

i) A Study of Preference Towards the Mobile Wallets Among the University Students in Lucknow City." *Scholedge International Journal of Management & Development ISSN 2394-3378* 4, no. 6 (November 27, 2017).

ii) Vijai, Dr C. "Consumer Attitude and Intention to Adopt Mobile Wallets in India." *Middle East Research Journal of Economics and Management* 1, no. 1 (December 25, 2021).

iii) Shukur, Mohammed H., Reem J. Ismail, and Laith R. Flaih. "Empower E-wallets Payment System by using A Hybrid Approach of Online and Offline Services." *Cihan University-Erbil Scientific Journal* 6, no. 2 (August 5, 2022).

iv) **“**Digital Payments in India: Background, Trends and Opportunities Hardcover – 1”, Jaspal Singh, New Century Publications, November 2019.

v) “Auth n Capture : Introduction to India’s Digital Payments Ecosystem Paperback”, 23 July 2021, Kindle Edition, ISBN-13 978-1639975136.

Dr. K. Sudheer Kumar

LESSON-10
SECURITY CHALLENGES IN MOBILE PAYMENTS

Learning Objectives

- ✓ To Discuss the Mobile payments
- ✓ To Know the Mobile Payment Security Measures
- ✓ To Understand the Mobile Payment Threats and Challenges

Structure

10.1 Introduction

The term ‘mobile payments’ refers simply to all payments that are made using your mobile device. Mobile payments include the use of mobile wallets and mobile money transfers. There are two types of mobile payments: online or in-app purchases, and using a POS terminal in a brick-and-mortar store.

The worldwide mobile payment revenue is expected to hit $12.06 trillion by 2027, with a CAGR (compound annual growth rate) of 30.1% from 2020 to 2027. The extraordinary growth in the mobile payments market can be attributed to the popularity of smartphones. The number of smartphone users worldwide is expected to grow by one billion every five years, which means that by 2023, the number of smartphone users is expected to reach 4.3 million.

In 2014, Apple launched Apple Pay which sparked the popularity of mobile payments and began a new era of convenience for consumers. More and more companies have joined this increasingly popular, competitive digital payments landscape including Samsung Pay, Android Pay and Google Pay (with the latter finally fully overtaking Android Pay's place). However, there are some concerns when it comes to the security of mobile payments

Processing payments is perhaps the most nerve-wracking aspect of running an ecommerce business. Not only does it keep your business's lights on, but it deals with sensitive customer information.

Most customers may believe the ecommerce payment process takes only a few seconds—as long as the click of a button. But it entails many points of communication between multiple players: customer, merchant, payment processor, merchant account service, and both the customer and the merchant's respective banks.

The rewards of choosing a payment processing solution that best fits your and your customers' needs can be major. Not only can you take in more money, but you can capture the 19% of users who are likely to abandon checkout because they don't trust a site with their financial information

Attributed to the popularity of smartphones, mobile payments have grown exponentially over the last few years. While smartphone users are expected to increase by 2 million every year, you can expect a compound annual growth rate of 30% in worldwide payment revenue alone with an expectation to hit $12.06 trillion by 2027!

As fraudsters become more and more advanced, now is the time to familiarize yourself with how to protect your personal information across all forms of technology. Just like how it's important to use good security safeguards when making purchases online, you should pay just as much attention to **mobile payment security threats and challenges**.

10.2 How to ensure payment security

The mobile payment space has rapidly accelerated. To protect yourself, begin by studying secure payment practices not only online, but also through your mobile devices as well. To help you get started, we'll cover the following in this guide:

- What constitutes a mobile payment and how do they work?
- Mobile payment security measures (tokenization and encryption)
- Are mobile payments actually secure?
- Top mobile payment security threats and challenges
- Products and features that protect from mobile security threats
- In-app payment security practices
- Which mobile payments are the most secure?
- The future of mobile payments

Armed with this guide, you can feel more confident about protecting yourself when making purchase decisions on your phone and combatting mobile payment security threats and challenges.

10.3 What are mobile payments, and how do they work?

"Mobile payments" refers to all forms of payments that are made through your mobile device including: mobile online browser, digital wallets, mobile money transfers, in-app purchases, and now with tap-to-pay / contactless options, and point-of-sale (POS) systems at brick-and-mortar stores.

Most mobile payments use a modern technology called Near-Field Communication, also known as NFC, that enables consumers and businesses to make and accept contactless payments.

When making contactless payments, you hold your mobile device near a POS terminal and NFC establishes a connection between your device and the terminal. NFC then uses close-proximity radio frequencies to send payment data from your phone to the card reader. Next, you may be prompted to validate your identity through a passcode, fingerprint, or other method. Once that's done, money is transferred from your bank account to the merchant.

10.4 Mobile payment security measures

Similar to traditional credit card processing, extra security measures are implemented to combat top mobile payment security threats. The following are a few safeguards mobile companies and devices put into place to mask and to protect sensitive cardholder data:

10.4.1 Tokenization

Tokenization randomly generates keys by replacing sensitive debit or credit card data with a unique code called a token. It often comes up in the context of contactless payments. At the point of purchase, a randomized 16-digit number is created by token providers, such as Visa and Mastercard, and the real number is stored in a secure vault. This token has limited validity: it cannot be used outside of the payment authorization process, and if intercepted, it becomes void.

NFC uses tokenization as soon as the connection has been established between your mobile device and POS terminals. NFC transmits the tokenized number to the merchant, which then sends this data over to the token provider, who confirms that the token matches the real credit card and approves the transaction in a few seconds.

10.4.2 Encryption

Instead of generating tokens, encryption uses a secret key to ensure private information is only accessible to the sending and receiving parties. Mobile devices rely on encryption to protect your data from falling into the wrong hands and to shield them from major mobile payment security threats. Without the right authentication key, the data is inaccessible even if the hardware is removed or placed into a different machine.

By default, most mobile devices are manufactured with some type of encryption programming, but you should research and confirm this before purchasing any type of mobile device.

10.5 Are mobile payments secure?

The short answer is, generally, yes.

Despite the rapid growth in mobile payments, there is still a predominant sense of uncertainty when it comes to the actual security of transferring and making payments through mobile devices.

According to a recent PEW survey, US consumers were more likely to believe that mobile payments were more "poorly protected" than paying with prepaid, debit, and credit cards. Even more so, for mobile payments that use a credit card, only 35% of consumers said that they were well protected compared to purchases made with a credit card on its own.

This uncertainty is understandable

Ironically, mobile payments can actually be more secure than regular payments, provided other key safeguards have been implemented. With safeguards such as tokenization and encryption in place across most mobile devices and payment companies, mobile payments by default have more security measures in place.

Say, for example, that you're paying for your goods at a convenience store and you're choosing to pay with your physical credit card versus a mobile payment option. If a bad actor had hacked into the store's POS system and you swipe your credit card, the bad actor could skim and steal your card information. If you instead choose to pay with mobile, the bad actor would not be able to easily decrypt the token. Consider that next time you're shopping in person

10.6 Mobile payments security threats and challenges

The biggest challenges and threats to mobile payments fall under these categories:

10.6.1 Personal lost or stolen devices

Losing a device or having it stolen happens more often than you might think. An estimated 70 million smartphones are lost each year, with only 7% of them recovered. And these days, smartphones act a lot like wallets since users store almost everything on their devices, from contact names, addresses, passwords, online banking apps, and mobile wallets. If your phone isn't properly protected, you risk having all of this private information stolen or leaked. We'll cover more on how to ensure your mobile device has all of the security measures needed should you ever lose your phone.

10.6.2 Using public and unsecured wifi

Online skimming can easily occur when fraudsters take advantage of unsecured wifi to steal a user's private information when shopping online. Bad actors will infect specific websites or unsecured networks with malicious code. They can gain access to payment pages where they can steal payment information like card numbers, CVV numbers, expiration dates, and more. Unfortunately, once the malware has been injected it is very difficult to trace, leading to unexpected or undetected fraudulent activity.

With that said, any time you are accessing private information such as bank information or making mobile payments online, make sure you are on a secure network first. Below are a few ways to make sure you are using a safe network:

- Use multiple firewalls. Firewalls are created to build a barrier between your network and any unauthorized users. Install a firewall on top of your antivirus software.
- Turn off your WPS (WiFi protected setting). The WPS is the function that lets devices like your phone and mobile devices pair with your internet network. This setting is convenient, especially when you have multiple devices, but it does leave large vulnerabilities for hackers to get in.
- Use a VPN (virtual provider network). VPNs hide your activity online so that no one can track what you're doing. This is a must-have when you're on a public network.

10.6.3 Late security updates

Users tend to delay software and mobile updates, which leaves them vulnerable to shifting mobile payment security threats. Typically, each update includes new security protocols and bug fixes built to safeguard attacks and the latest vulnerabilities. Despite this, according to a study by The Journal of Cybersecurity, only 54% of participants actually updated their software, and 65% of those updates were delayed.

In 2017, around a quarter of a million Windows computers around the world were infected with malware "WannaCry". The victims were locked out of their computers, and the only way to regain access was to transfer $300-$600 worth of Bitcoin to the fraudsters. This could have been wholly prevented had the affected updated their software on time.

Software updates can sometimes take a few hours to complete, but it's in your online security's best interest to do them as soon as you can. And be sure to have them updated as soon as possible across *all* mobile devices - including tablets and laptops - so that any malware can't be leaked cross-platforms.

10.6.4 Phishing scams

Fraudsters can easily tap into phishing scams on mobile devices. If you see a sketchy email, be wary of the email's sender, formatting, potential spelling errors, and other red flags. If something seems off, don't click anything. Bad actors often take advantage of smaller mobile screens to hide malicious links and pop-ups.

Likewise, mobile phishing scams can also come in the form of texts and app notifications. If you see a text from someone you don't recognize, don't click it. Instead, delete it immediately. Clicking into a malicious link could result in unintentionally downloading bad software onto your device.

10.6.5 Weak passwords

Easily, the most common way that fraudsters get a hold of private information is through hacking weak passwords. For all accounts that are accessible through your mobile device, make sure you have used a password generator, such as 1Password, to ensure that your passwords are strong. And, of course, make sure you never carry your phone around unlocked.

10.7 Products and features that protect from mobile security threats

In addition to what you should watch for when making mobile payments, there are products and features you should add to your security toolkit.

How to make sure your phone is secure

Beyond regular software and security updates, there are a few options you can enable on your mobile device for added security.

- **Set up all locked security features.** Beyond the phone password, don't ignore the other security benefits that most mobile devices offer such as facial recognition, iris scans, and fingerprint recognition. These were created to help you!
-
- **Set up 2FA.** Two-Factor Authentication (2FA) is a security measure that prompts users to verify their identity in two different ways. In most cases, this will be an account password plus a code sent to an email address or phone number. 2FA makes it more difficult for hackers to access accounts as it requires another device login outside of just a password. Make sure that 2FA is turned on for all accounts that your mobile device is linked to, including email, sensitive work documents, and financial accounts.

  Set up Find My Phone. If your phone is lost or stolen, you can use this to locate your device. If there are any suspicions that the phone has been stolen, take action immediately. Close your cards and change the login information on all of your high stake accounts that are connected to your mobile device.

  Familiarize yourself with your rights. Since 2018, the Technological Advisory Council (TAC) reported that all phones manufactured after 2015 would enable users to:

  Remotely wipe the authorized users' data (such as contacts, photos, and emails) from the smartphone if lost or stolen.

  Render the smartphone inoperable to an unauthorized user, such as locking the smartphone so it can't be used without a password.

  Prevent reactivation and any kind of hard resets without the authorized user's permission.

  Reverse inoperability if the smartphone is recovered.

Most mobile companies have added this to their product safety guardrails to prevent common mobile payment security threats. If you have an iPhone, you can access "Lost Mode". Lost Mode locks your iPhone and Apple devices so that others can't access your personal information. It will also display a phone number and a message on the screen so that if someone finds it, they will be able to contact you and nothing else. If you didn't have a passcode set up, this option will prevent your iPhone from being unlocked. Likewise, if you have an Android, you can use Android Device Manager to locate a lost or stolen phone.

10.7 .1 Use a virtual card when shopping on mobile (plus a travel hack!)

In spur of the moment events - whether you are purchasing tickets last minute or accessing your bank account when you're on the go - online skimming can happen.

If you are in need of making an emergency purchase when you're on unsecured wifi, we strongly suggest you use a secure virtual card like the ones offered by Privacy. You can generate a virtual card on the go, and create a Single-Use Card that will automatically close two minutes after the transaction goes through.

For example, say that you are traveling abroad and in need of buying train tickets while on the move. When connected to the public wifi, simply go into your Privacy app, generate a card, and use the one-time number at checkout. If a bad actor somehow gets a hold of this information, they won't be able to access this payment method. You will even be notified if someone attempts to do so.

We also recommend using this strategy for all of your mobile purchases. Consider designating Privacy Cards strictly for your phone purchases via apps and online.

10.8 Practice online shopping safeguards, even on mobile

Follow the same online shopping security practices as you do when making purchases online. Mobile payment security threats occur just as frequently through purchases that are made on a mobile web. Refer to our guide that covers all the basics you need to know to prevent online shopping fraud, including mobile purchases.

10.9 In-app payment security practices

Apps are a common place that bad actors access. If you are making purchases through an app, follow these guardrails:

1. **Use a trusted platform and conduct due diligence**

   If you are going to add payment information to your smartphone, always make sure that you're using the most updated version of a trusted third party vendor. Read through the privacy policies, make note of how many times the app has been downloaded, read the reviews to learn about other users' experiences, and make sure that the permissions that you are granting the app are appropriate to what you are using it for. For instance, there's no need for a banking app to have access to your text messages.

2. **Set up payment notifications across all your apps**

   App notifications can be annoying for some, but not when it comes to your payments. Once enabled, you can be alerted each time a transaction is made. And if it's unauthorized, you can handle it immediately. Similarly, if you are sending money to a friend, you can quickly confirm whether the transaction went through or not.

3. **Enable automatic app updates**

   Similar to making sure that your mobile device software is up to date, automatic app updates will activate each time the relevant app is upgraded with security enhancements and bug fixes. This is an easy way of managing your apps and making sure that evolving mobile payment security threats are addressed.

4. **Use QR codes when possible**

For peer-to-peer money transfers, always look up a user's QR code, instead of typing in a user name when sending cash. It's not uncommon for scammers to impersonate someone you may know by changing their profile picture and creating a similar username. In the case of any typos, duplicate fraudulent accounts, or phishing accounts, looking up a user's QR code will guarantee that you are sending payments to the account you intend to.

5. **Hide your transaction activity**
   Some payment apps thrive on the social connectivity between friends and your community. For example, on Venmo, you can see transaction activity between your friends, and even engage with them with likes and comments. However, to stay vigilant, we recommend that you hide your footprint, including your friends lists. Not everybody needs to see your business - and in the long run, you will be protecting yourself and your contacts from any malicious outside parties.

10.10 What mobile payments are the most secure?

There are a variety of different mobile payment options available, but these are the most popular:

1. Apple Pay
2. Google Pay
3. PayPal
4. Square
5. Venmo
6. Zelle

If data privacy is your biggest concern, choose apps from Apple or Google in general. Separately, if avoiding sending money to the wrong person is a higher priority, select payment apps that let the recipient use a QR code or shared link, such as PayPal, Square, or Venmo. Regardless of which payment method you choose, each has its pros and cons when it comes to fighting mobile payment security threats.

Across the board, all the listed apps have a bounty net program in place, which allows users to report scams or exploits in exchange for cash. This incentivizes users to take notice of malicious behavior and reduce fraud. Additionally, every app also has a method of passcode-locking to prevent unauthorized users from initiating a payment without you. If a bad actor got ahold of this app, they wouldn't be able to use it without your passcode.

On the flip side, unfortunately none of the apps offer compensation for fraud losses on personal transactions. If you accidentally fall for a scam, for example, there generally is not much you can do to recover your losses from the company behind an app.

When it comes to data privacy, all of these payment apps share some level of personal information with third parties, such as banks or fraud-monitoring services. However, Google and Apple generally do not go beyond what is required for transaction approvals. Others like Square, Venmo, and Zelle do sell data for marketing purposes, so you may want to keep that in mind when you're making transactions using these services.

10.11 The future of mobile payments

As consumers have quickly adapted to an environment where cash is no longer king, the rise of mobile payments will undoubtedly continue to develop and accelerate. The convenience and accessibility they bring will ensure that they remain a consumer staple.

Beyond mobile wallets, contactless payments, and the rise of smartphone apps, other alternative payment platforms will begin to be more widely accepted, such as cryptocurrency. In fact, according to a Deloitte survey, 75% of US retailers plan to accept payments in crypto within the next two years. Several NFL athletes have already accepted crypto over cash salaries, and a region in Switzerland even accepts Bitcoin and Ethereum as tax payment methods. Mobile payments are just the tip of the iceberg of how consumers will be able to make payments in the future.

As fraudsters become more tech savvy, it's important to practice all the security safeguards needed when making purchases online, through phone, and via alternative payment methods. Mobile security threats and challenges will continue to evolve as fraudsters continue to become more nimble. Armed with the right practices and knowledge, however, you can feel secure when making all of your purchase decisions.

10.12 Mobile security checklist

We covered a lot in this guide, so we created a quick checklist to ensure that you are properly protecting yourself from mobile payment security threats and challenges.

General

- Set all security passwords on your phone - including phone lock, face recognition, and fingerprint accessibility, if available. If your phone is lost or stolen, your data is protected.
- Make mobile payments only when you are on a secure wifi network. If you absolutely need to make a purchase when you are not on a secured network, consider using a virtual card provider, such as Privacy, that has a Single-Use payment option. As soon as the transaction goes through, the card will automatically close so it cannot be used anywhere else.
- Make sure that all of your mobile devices have the latest software update installed.
- Be wary of phishing scams. If you see a sketchy email or text from an unrecognized user, do not click into it and delete immediately.
- Use a secure password generator for all accounts that your mobile device is connected to.

For your phone

- Double check that all security features have been enabled.
- Set up 2FA on all accounts that are connected to your mobile device.
- Enable "Find Your Phone".
- If you have an iPhone, use "Lost Mode" if your phone has been lost or stolen. On Android, use the Android Device Manager. Regardless of device type, understand that you have the legal right to protect your mobile data, as covered by the TCA.

For phone apps and in-app purchases

- Do proper due diligence on payment apps you're looking to download. Things to check include the privacy policies, how many times it has been downloaded, and reviews. Only enable access to data to pieces that are appropriate for the app.
- Turn on payment notifications. Confirm every time a transaction has gone through, and be notified immediately if a payment is unauthorized.
- Enable automatic app updates. Similar to device updates, make sure that your apps are up to date with the latest security protocols and bug fixes.

- For peer-to-peer payment apps, use QR codes to look up the recipient. Typos can easily occur and fake duplicate accounts from scammers are common. QR codes will guarantee that you are sending the transaction directly to the recipient you intend to.

10.13 Summary

The demand for debit and credit cards has also seen a steady rise over the last few years. Most of the banks now provide online banking and debit card facility with every new account. With the financial inclusion drive by the RBI, the number of bank accounts (and hence the number of debit cards) will definitely see a rise. This coupled with rising disposable income will invariably lead to more online transactions**.**

10.14 Key words

Mobile Payments- The term ‘mobile payments’ refers simply to all payments that are made using your mobile device. Mobile payments include the use of mobile wallets and mobile money transfers

Tokenization-Tokenization randomly generates keys by replacing sensitive debit or credit card data with a unique code called a token. It often comes up in the context of contactless payments.

Encryption- Instead of generating tokens, encryption uses a secret key to ensure private information is only accessible to the sending and receiving parties. Mobile devices rely on encryption to protect your data from falling into the wrong hands and to shield them from major mobile payment security threats

Phishing scams- Fraudsters can easily tap into phishing scams on mobile devices. If you see a sketchy email, be wary of the email’s sender, formatting, potential spelling errors, and other red flags. If something seems off, don't click anything. Bad actors often take advantage of smaller mobile screens to hide malicious links and pop-ups.

10.15 Self Assessment Questions

1. Briefly Explain the Mobile Payments
2. Discuss the Mobile Payment Security Measures
3. Critically explain the Mobile Payment Threats and Challenges

10.16 Suggested Readings

1. Engel-Flechsig, S. 2001. Securing the new global economy, Mobile Commerce World.

2. Au, Y.A. & Kauffman, R.J. (2007). The economics of mobile payments: Understanding stakeholder issues for an emerging financial technology application, Electronic Commerce Research and Applications

3. Tiwari, R., and Buse, S. 2007. The Mobile Commerce Prospects: A strategic analysis of opportunities in the banking sector (PDF). Hamburg: Hamburg University Press.

4. Pousttchi, K., Schiessler, M., & Wiedemann, D. G. (2007). Analyzing the Elements of the Business Model for Mobile Payment Service Provision, Management of Mobile Business

5. Pandey, S. (2013, April 23). Airtel Money. (G. S. Sambhy, Interviewer) Mumbai, Maharastra, India.

Dr. Ch. Prasad

LESSON-11
ELECTRONIC INVOICE PAYMENT SYSTEMS

Learning Objectives

To Briefly Explain the Benefits of an EIPP
To Discuss the Data elements in EIPP
To Describe the Benefits of Streamlining Payment Process

Structure

11.1 Introduction

EIPP stands for Electronic Invoicing Presentment and Payment and is a type of software used by finance teams for accounts receivable management. With an EIPP, companies can automate the process of emailing invoices and account statements in bulk to their customers when it’s time for them to pay their bill. (That’s the Electronic Invoicing Presentment part of EIPP.) EIPP software also includes an online payment portal that enables companies to accept payments on those invoices from their customers (hence, the Payment part of EIPP).

11.2 Benefits of an EIPP

EIPP software can greatly improve a company’s efficiencies and optimize its invoicing and payment processes, as electronic invoicing (e-invoicing for short) can save both time and money for companies - as well as improve their customers' experience.

11.2.1 Time Savings

It takes a lot of time for someone to print invoices and mail them via the US Postal Service. It also takes a lot of time for someone to email monthly invoices to customers one by one. Nor is it sustainable to receive bank payments with disconnected remittances. Automating this process greatly reduces the time spent on manual work, allowing employees to focus on more important tasks. In addition, automated e-invoicing reduces the chance for human error (such as accidently notifying customers that don't have an upcoming payment, notifying the branch office contact instead of the headquarters, or forgetting to attach the invoice). This also saves time that would be otherwise spent on corrections.

11.2.2 Money Savings

It's also more expensive to print invoices and mail them via the US Postal Service and accept payments from fragmented channels. Automated e-invoicing reduces paper and postage costs and helps companies along their path to going paperless. Working to eliminate paper invoices, manual data entry, and fees from multiple payment channels can reduce costs for a company in the long run.

11.2.3 Improved Customer Experience

On the B2B payments side of an EIPP, online bill pay also improves the customers' experience by making it easier to do business with their company. Their customers don't have to tear remittances off the paper invoice, stuff them in envelopes, or mail checks at all. They simply click on the "pay now" link in an email – which can help them get paid faster. If customers have a question about their bill, they can message the vendor directly in the portal if they prefer e-communication over phone calls.

11.3 Consider to Choosing an EIPP

Many software providers offer an EIPP as part of their larger accounts receivable automation platform. When choosing an EIPP for your business, consider the following questions:

- Is it Easy to Integrate?
- Is it Customizable?
- Is it Secure?

11.3.1 ERP Integration

Enterprise Resource Planning (ERP) systems are a core system for accounts receivable teams, but they tend to offer limited automation. Therefore, the expanded functionality that an EIPP provides can be appealing. Of course, EIPPs were designed to integrate with ERPs and their add-on modules for accounts receivable management, but some integrations can be difficult. Therefore, it's important that any middleware or bolt-on software such as an EIPP be easy to integrate and interconnect with multiple ERP systems to better achieve process efficiency and truly optimize its invoicing and payment processes.

A/P Portal Integration

An EIPP benefits not only accounts receivable teams, but accounts payable (A/P) teams as well. A/P portals are becoming a common method of how large enterprises choose to receive invoices. For companies that serve larger enterprises, A/R teams might need to do more than send an email and expect a prompt payment. Even though there are electronic data interchange (EDI) standards that most portals support, each vendor portal and implementation is unique and needs a configurable solution. A/R teams that spend additional time posting invoices to customers' A/P portals, some of which specialized by industry (retail, for example), can greatly benefit from the automation that an EIPP provides.

11.3.2 Is it Customizable?

Companies also might want to consider some level of customization for their online payment portal so that the platform does (and looks) exactly like they need it to. Some vendors provide this as part of the platform, while others charge additional fees for any customization. A platform that allows you to easily add your company's logo and other branding requirements is helpful in providing a consistent and authentic user experience for your customers. Configuration is also helpful in how your customers can use the platform. Can the user set up payment plans? Access historical statements? Track new orders? Communicate with you? A platform that has limited capabilities – such as only accepting credit card and ACH payments and current statements – may not have the flexibility that your company needs. You may need to support multiple standard banking formats such as ACH, SWIFT, and EFT.

11.3.3 Is it Secure?

Finally, security is top of mind for any B2B payments software implementation. Companies should search for a secure, end-to-end connection accessible for both small and large customers that provides straight-through processing between the customer's and the supplier's systems. When choosing an EIPP platform, consider if the vendor is PCI (Payment Card Industry) compliant or works with a third-party PCI compliant payment processer.

EIPP Directory Providers are responsible for the message routing, for storing Payees' data and making them available to potential Payers for initiating EIPP related flows. The sources of data to be inserted in EIPP Directories are the EIPP Service Providers of Payees and data is sent via the Enrolment message so that, by making use of Directory Providers, they can inform the EIPP eco-system about the enrolment of a Creditor/Payee. The 2018 EIPP MSG report provides detailed functional specifications of Enrolment message including what requirements should be fulfilled in the implementation of the standardised messages. After initial analysis built upon the already delivered functional design, it was proposed that the Enrolment message should be composed of the following main components:

- A Header, composed of technical information about the message itself such as identifier, creation time, initiating and receiving parties.
- A Creditor Enrolment part, providing information about the Payee/Creditor subject to Enrolment, mainly its identifiers, names, addresses, and specific elements allowing functions such as: enrolment start and end time, the visibility of the Payee, what type of Activation the Payee allows.

A section containing indications for Activation Data, including what types of information the Payee expects from the Payers within the Activation messages.

- A section for Supplementary Data, a placeholder for any additional data that might be necessary during the exchange of enrolment message.

11.4 Data elements in EIPP

1.Start Date and Time and End Date and Time: to be used when a Payee limits the time period in which it can receive service activations requests and send RTP accordingly. If not used, the Payee can receive activation requests and send RTPs as of the time when its data are inserted into the EIPP Directories.

2. Limited Visibility: if set to FALSE or absent, the Payee is fully visible, i.e. its data can be retrieved by the Payers via available tools offered by Payers' EIPP Service providers by querying EIPP Directories. The specification of these queries is currently out of scope of this MSG. If

Limited Visibility is set to TRUE, the Payee data stored in EIPP directories should not be accessible to Payers by making use of queries.

3. Service Activation Allowed: if set to FALSE, the Payee cannot receive EIPP activation messages from the EIPP eco-system, but only using different alternative activation methods.

4. Creditor Service Activation Link: to be used to indicate a reference to an alternative activation method provided directly by the Payee in case Service Activation Allowed is set to FALSE. Other information regarding the use of Enrolment messages or of its data elements can be found in the detailed Message Definition Report (MDR), document required for submission to ISO 20022 of the message creation request.

Activation message

It was accepted that the RTPs containing e-invoices can be sent by Payees only if they have previously received the consent from Payers. This consent could be delivered with the Activation message that has two purposes: to communicate the consent of the Payer to receive RTPs from this specific Creditor/Payee and to communicate to the Payees the identity of the Payer along with its "EIPP address" i.e. the identifiers of the Payer's EIPP provider and of Payer itself accordingly. To send an Activation request to a Payee, the Payer needs to know the Payee identity and the Payee "EIPP address". Such information can be obtained by querying EIPP Directory Providers or could be received directly from the Payee. The 2018 EIPP MSG report provided detailed functional specifications of Activation messages including the requirements that implementations of the message in a standardised framework should fulfil [ref needed]. The following main components should be included in the Activation messages:

• A Header, composed of technical information about the message itself such as identifier, creation time, initiating and receiving parties.

• A Debtor Activation part, providing information about the Payer/Debtor and the corresponding Payee/Creditor related to the EIPP service Activation, mainly their identifiers, names, addresses, and specific elements allowing functions such as: activation start and end time, information needed by the Payee to correctly perform the activation in its systems such as a contract reference or a dedicated activation code.

• An E-invoice Data part containing indications that the Payer can communicate to Payee in relation to E-invoices included in RTPs.

• A section for Supplementary Data, a placeholder for any additional data that might be necessary during the exchange of activation message. Further development of an EIPP scheme and specifications for implementation should take into account the following requirements:

1. Activation messages requests can be sent only to Enrolled Payees.
2. If the Payee limited visibility indicator is set to FALSE in the Payee Enrolment data, the Payer's EIPP provider can retrieve the Payee data required for activation by querying the EIPP Directory Providers. 3. If the Payee limited visibility indicator is set to TRUE, the Payer may use the data element Dedicated Activation Code in the Activation message request. This code, specific to each Payer and to each Activation, should be communicated by the Payee to the Payer prior to Activation. The mechanism for the creation and communication of this code would be outside of the EIPP rules.

3. If the data elements Start Date and End Date are used, the Payee receiving the Activation request message should record the activation as active only within the time period indicated by these elements so that RTPs cannot be sent outside this period. Other information regarding the use of Activation request messages or of its data elements can be found in the

detailed Message Definition Report (MDR), which is the document required for submission to ISO 20022 of the message creation request.

4. ISO 20022 for servicing messages

ISO 20022 has been identified as the suitable standardisation framework for the Enrolment and Activation messages (request and status report), due to the close relation with existing ISO 20022 RTP message and in general with messages from the SEPA Payment schemes which rely on ISO 20022 Payments domain messages. After analysis of the existing ISO 20022 messages set, the MSG concluded that no existing message can fulfil the requirements for EIPP Enrolment. Therefore, it was decided to submit the Request for the creation of a new set of ISO 20022 messages. The high-level structure of messages should match with the sections described above and exiting data elements from other types of messages will be as much as possible reused. Corresponding messages for unenrolment, amendment of an enrolment, deactivation and amendment of an activation are also proposed.

5.Extension of servicing messages functions

In the course of the work on designing the servicing messages dataset, some communities considered that there is a need in the market for extending the functions that Enrolment and Activation should support, as follows:

- In the current design, only Payees can be enrolled in EIPP Directories. The identified extension is that in the Business-to-Business context only, it would be useful that companies acting as Payers can be also enrolled in EIPP Directories, so that they can show or display within the EIPP eco-system their availability to receive RTPs/E-invoices from Payees.
- In the current design, through the EIPP eco-system, Activations are possible only from Payers. The identified extension is that Payees can also initiate Activations, provided that the Payers give their consent of receiving such requests through alternative ways. The EIPP MSG recognised the market needs expressed in these possible extensions, but concluded that including them in the current design requires further analysis, which is beyond the EIPP MSG

11.5 EIPP – The Ultimate Payment Process

Today's EIPP (Electronic Invoice Presentment and Payment) solutions take the invoice from submission to the appropriate payment, from ACH with dynamic discounting for discount maximization, to card processing for increased days payables outstanding, to check printing. All of these functions make EIPP the ultimate payment process! They allow B2B transactions to take place with better efficiency than ever before.

It is interesting, that with the expansion of payables automation and EIPP, there are so many solutions that just can't offer the payment portion. **IPAYABLES**, an industry leader in EIPP, has expanded their payment options with a wide range of choices including: Customer System Delivery, ACH Transaction, American Express P-Card, MasterCard P-Card and Check Printing. iPayables also provides remittance detail to the supplier for purposes of cash application and reconciliation. It is interesting that so many of the payables automation solution providers stop prior to the payment step.

Here is a review of some of the payment processes you would expect to see in electronic invoice presentment and payment:

11.5.1 Customer System Delivery

This is where the electronic invoice is simply delivered to the customer to pay withing their system. It is commonly available withing their system. It is commonly available with most any automation solution.

11.5.2 Ach With Dynamic Discounting

Most companies are familiar with ACH, but there are challenges in collecting banking information from suppliers. This may be why many payables automation providers stop short of payment. iPayables and most EIPP solutions that perform ACH transactions are collecting ACH related information online and most often following up with phone calls to retrieve or validate information. Aside from the convenience of the EIPP provider collecting this information, the greatest benefit of all could come from enhanced control over payment timein. According to the procurement trand publication *Spend Matters*, businesses can earn a 20 percent or greater annual return on their invested capital by making early payments to suppliers. With dynamic discounting, the customer is using their working capital to pay suppliers early, but they are collecting a great return on that investment in the form of high value discounts.

11.5.3 Payment Cards (Purchasing Cards)

For customers who don't have the working capital to do early payments themselves, iPayables recommends using purchasing cards as a strategic form of payment for accounts payable. Purchasing cards processed through iPayables net the customer a handsome rebate, but actually extends the payment terms. Suppliers are often willing to take purchasing cards as payment for early payment when an early payment from the customer is not available.

11.5.4 Automated Check Payment

Though a customer may want all payments paid electronically, there will often be some portion left as check. These can be managed with customer system delivery, or companies like iPayables will print the needed checks. This all-in-one approach allows the customer to focus on the supplier relations, audit and other value add efforts and not on paper printing.

A recent 2013 study by AFP the Association of Financial Professionals found that, "78 percent of organizations have integrated their ACH systems with accounting while 56 percent have done so for card payments," said Jim Kaitz, AFP's president and CEO. "AFP strongly supports electronic payments and we're pleased to see the payment innovations now available to corporate treasurers."

Improved technology and automation provide businesses with more choices when it comes to improving and expediting payment methods. The trend towards more flexibility and higher consumer demand has made traditional payment methods obsolete. Not only has there been a payment/ automation change in B2B, there has also been a methods change. EIPP with ACH and Dynamic Discounting is the latest evolution in payment processing, and it has become a popular and readily available option in accounts payable processing.

11.6 Benefits of streamlining payment processes

1. Enhanced customer experience

Remember that feeling when you strolled into a store, eyes lighting up as they landed on that thing you just had to have? You made a beeline for it, went to pay, and voilà, everything went off without a hitch. You walked out, a little pep in your step, feeling like you owned the world.

That's the enchantment of flawless transactions. When payments feel like a waltz rather than a hurdle, customers don't just feel like another number; they feel cherished. It's this silent connection that keeps them coming back, drawn like a moth to a flame.

2. Reduced cart abandonment

Picture a virtual shopper, balancing a steaming mug of tea, navigating your online store. Their cart's full, but one hiccup in the payment process? They're out quicker than you can say "checkout."

Simplifying this delicate dance keeps them twirling in your digital aisles, ensuring that dance doesn't turn into a hasty exit. Moreover, a streamlined process can significantly improve the conversion rate, driving more sales from the same amount of traffic.

3. Efficient operations

Navigating each transaction is like untangling a ball of yarn; every knot you free up gives you that extra second to weave something beautiful, unleash a burst of creativity, or even just kick back with a soul-soothing cup of joe.

By smoothing out your payment processes, you're not just tidying up the paperwork; you're sprinkling a little zest and zeal into your team's everyday hustle.

4. Heightened security

"Security in today's digital world isn't just a technological requirement; it's a trust pact you make with your clients," says Mark Pierce, CEO of Cloud Peak Law Group.

"When you safeguard transactions with the latest encryption tools and multi-factor authentication methods, you're not merely keeping data safe; you're making an unwavering commitment to your client's peace of mind and the integrity of your services."

Real-time Reporting: Imagine having a crystal ball that offers insights into your transactions, whispering tales of customer behavior and unfolding market trends. That's what modern, streamlined processes offer—data-rich narratives that help pen your business's future chapters.

5. Cost savings

Sure, there's a little bit of money spent in refining the payment system initially, but think about the treasures you'll amass in the long run! From fewer coins lost to transaction fees to saving the golden goose with fewer chargebacks, it's a bounty waiting to be claimed.

6. Environmental benefits

A streamlined process often nudges you to embrace the digital realm. This wins you points with Mother Nature for reduced paper trails and paints your business green in more ways than one.

11.7 Streamlineof payment processes

Navigating the vast ocean of payments can feel like being a sailor amidst a choppy, unpredictable, and demanding storm. Yet, just as a seasoned sailor knows how to harness the wind, mastering the art of payment processes can be your compass to smoother financial shores. Embarking on this journey requires meticulous planning and execution.

Here's a detailed treasure map to ensure you navigate this realm adeptly:

11.7.1 Assessment of current systems

A holistic assessment of your present payment system forms the streamlining foundation. Dig deep into the nooks and crannies.

How long does an average transaction take? Are there any recurrent issues that customers or employees report? What's the feedback loop like? Knowing these can highlight inefficiencies that may have been invisible at a surface glance.

Linda Shaffer, Chief People Operations Officer at Checkr, adds, "Once the examination is complete, create a detailed report or dashboard. This visualization will clarify the pressing issues and offer a baseline against which to measure future enhancements. Setting benchmarks now will assist in tracking improvements as you advance in the streamlining journey."

11.7.2 Adoption of integrated payment solutions

Imagine isolated payment systems as far-flung islands in a vast sea. To ensure your revenue flows smoothly like a steady current between these islands, you need sturdy bridges. That's where integrated payment solutions come into play, linking these islands together.

When these systems chat and collaborate like old friends, you sidestep the pitfalls of data being trapped in lonely corners, mixed signals, and frustrating lags.

Eric Mills, Owner of Lightning Card Collection, paints a clearer picture. "It's not just about lumping systems together. It's about creating a symphony where each part complements the other. Opt for solutions that gel with your current setup but also jazz it up. This might mean saying goodbye to some outdated tools or welcoming sleek, new platforms that can groove with your business's ever-evolving rhythm."

11.7.3 Regular training and skill upgrade

Diving into the whirlwind world of payment technology is like mastering a salsa dance - every step is crucial, and the rhythm keeps changing!

As fresh moves (or innovations) pop up almost magically, it's vital to keep your team dancing in sync. Regular jam sessions (or training) are the key! But it shouldn’t be about just memorizing the steps; they need to feel the beat and groove with it.

Tom Golubovich, Head of Marketing & Media Relations at Ninja Transfers, chimes in, "Always remember, a crew that dances with confidence moves fluidly and flawlessly. So, once they’ve got the basics, give them the stage to freestyle. Encourage them to explore - maybe through some cool online dance tutorials, interactive webinars, or immersive workshops. The aim? To make sure they not only follow the beat but sometimes even set it!"

11.7.4 Implementing automation

Time is a resource more precious than gold in the world of business. Why spend it on tasks that machines can do faster and more accurately? For instance, Helcim's recurring billing tool is a beacon of automation excellence.

This tool not only manages regular billing cycles but can also be seamlessly coupled with invoicing and ACH transfers, which have the advantage of lower processing fees. Such tools ensure timely payments, reducing the administrative burden and providing a cost-effective solution.

Automation isn't about replacing the human touch but enhancing it. With repetitive tasks taken care of, such as those managed by Helcim's tool, your team can focus on strategic decision-making and enhancing customer experiences.

Stephan Baldwin, Founder of Assisted Living, emphasizes, "While automating, it's essential to maintain a balance. Automate where it makes sense, ensuring you're not depersonalizing essential touchpoints. The goal is efficiency without compromising on the quality of interaction."

11.7.5 Ensuring secure transactions

Much like the vast seas, the digital realm is replete with threats lurking in the shadows. Protecting your treasure—customer data and financial information—is paramount, especially when accepting online payments.

Prioritizing robust security protocols is not a luxury; it's a necessity. This involves multi layered security measures, regular updates, and adhering to industry-standard compliance regulations.

"Besides the technical aspects, educating your team and customers on best practices is vital. Ensure they know common threats and the steps they can take to safeguard themselves. After all, a vigilant crew and an informed clientele form the first line of defense against potential breaches." - Volodymyr Shchegel, VP of Engineering at Clario.

11.7.6 Feedback Collection and Continuous Improvement

Imagine sailing without ever consulting the stars or the winds. Feedback from stakeholders—be it customers, employees, or partners—is that guiding star in the realm of payment processes.

Proactively seek it, cherish it, and act on it. It offers a perspective that you, engrossed in the intricacies of operations, might miss.

Fernando Lopez, Marketing Director at Circuit, adds, "Collecting feedback is only the first step. Analyzing it, identifying patterns, and iterating based on it is where the magic happens. Adopt a culture of continuous improvement, where feedback isn't seen as criticism but as an opportunity to refine and enhance. With each iterative step, your processes will become more streamlined, efficient, and user-friendly."

11.8 Summary

As a business, you're not just crunching numbers or making transactions; you're crafting unforgettable experiences. For your venture to soar, your payment methods need to sway effortlessly to the tune of today's digital dance: quick as a flash and solid as a rock.

11.9 Key words

Payment Cards (Purchasing Cards)- For customers who don't have the working capital to do early payments themselves, iPayables recommends using purchasing cards as a strategic form of payment for accounts payable

EIPP (Electronic Invoice Presentment and Payment) solutions take the invoice from submission to the appropriate payment, from ACH with dynamic discounting for discount maximization, to card processing for increased days payables outstanding, to check printing

11.10 Self Assessment Questions

1. Briefly Explain the Benefits of an EIPP?
2. Discuss the Data elements in EIPP?
3. Describe the Benefits of Streamlining Payment Process?

11.11 Suggested Readings

1. Engel-Flechsig, S. 2001. Securing the new global economy, Mobile Commerce World.
2. Au, Y.A. & Kauffman, R.J. (2007). The economics of mobile payments: Understanding stakeholder issues for an emerging financial technology application, Electronic Commerce Research and Applications
3. Tiwari, R., and Buse, S. 2007. The Mobile Commerce Prospects: A strategic analysis of opportunities in the banking sector (PDF). Hamburg: Hamburg University Press.
4. Pousttchi, K., Schiessler, M., & Wiedemann, D. G. (2007). Analyzing the Elements of the Business Model for Mobile Payment Service Provision, Management of Mobile Business

Dr. Ch. Prasad

LESSON-12
E-INVOICING

Learning Objectives

To Discuss the E-invoicing Work
To Describe the Benefits of E-invoicing work
To Know the difference between an invoice and an e-invoice
To Understand the Guidelines of the Electronic Invoicing

Structure

- 12.1 Introduction
- 12.2 How Does E-invoicing Work?
- 12.3 Uses of E-invoicing
- 12.4 Benefits of E-invoicing
- 12.5 What's the difference between an invoice and an e-invoice?
- 12.6 How does e-invoicing work
- 12.7 How do I send an e-invoice
- 12.8 When is e-invoicing required?
- 12.9 E-invoicing can help close the VAT gap
- 12.10 How can e-invoicing impact my business?
- 12.11 What are the benefits of e-invoicing for my business?
- 12.12 How can e-invoicing improve my cash flow?
- 12.13 How do I transition to e-invoicing?
- 12.14 Guidelines of Electronic Invoicing
    - 12.14.1 Electronic Invoicing
    - 12.14.2 Tax Invoice
    - 12.14.3 Simplified Tax invoice
    - 12.14.4 . Electronic Note:
    - 12.14.5 Debit Note
    - 12.14.6. Credit Note
    - 12.14.7. E-Invoice Solution
    - 12.14.8. FATOORA Portal
    - 12.14.9. Cryptographic Stamp
    - 12.14.10. Cryptographic Stamp Identifier (CSID)
    - 12.14.11 UUID
- 12.15. FATOORA Portal
- 12.16. Cryptographic Stamp
- 12.17. Clearance
- 12.18. Reporting of Simplified Tax Invoices and their associated notes
- 12.19. Human Readable Format
- 12.20. The Authority's Toolkit
- 12.21 Types of E-Invoices
    - 12.21.1. Tax Invoices for Phase 1 (Generation Phase)
    - 12.21.2. Tax Invoices for Phase 2 (Integration Phase)
    - 12.21.3. Simplified Tax Invoice
    - 12.21.4. Simplified Tax Invoices for Phase 2 (Integration Phase)

12.1 Introduction

Electronic invoicing (e-invoicing) is the electronic exchange of an invoice document. This takes place between buyer and supplier. In the past, invoicing has involved a lot of manual labour and is vulnerable to human error. This can increase costs and lengthen processing times for businesses.

E-invoicing makes use of a variety of tech and entry methods. It is often used as a catch-all word to denote any approach to presenting an electronic invoice to a client for payment.

E-invoicing is not a brand-new concept. Electronic data interchange (EDI) and XML formats have been in use for electronic invoices for 30 years. Recently, the government has been the primary force driving the adoption of e-invoicing.

The pandemic served as the driving force for some procurement firms to adopt touch-free technologies. E-invoicing is a good example of these technologies.

12.2 How Does E-invoicing Work?

An electronic invoice is one that you create, transfer, and receive digitally. The legitimacy and content of an electronic invoice are the same as those of a paper invoice. You may use different data formats to represent and transfer an electronic invoice.

Recipients must enter invoices digitally into the company's system before processing payments. Invoices are still printed on paper, placed in envelopes, franked, and despatched with hefty postage. This manual process is expensive in terms of both labour and time.

The best way to differentiate what e-invoicing is to follow these rules.

E-invoicing is:

- Electronic Data Interchange (EDI) or XML-formatted structured invoice data
- Structured invoice data supplied through common online forms on the internet

E-invoicing is not:

- Unstructured bill data in Word or PDF formats
- Paper bills sent with fax machines
- Paper invoices that you scan

12.3 Uses of E-invoicing

Using e-invoicing allows companies to receive invoices from many vendors. This can include formats like image-based invoices.

You can use one platform for managing all info and tasks related to accounts payable. There is no content duplication when business users effortlessly access, sync, and aggregate data. This is across numerous systems and devices.

E-invoicing is crucial for helping businesses streamline their invoice processing cycles. It helps businesses lower the amount of time spent on processing, approving, tracking, and chasing down invoices. E-invoicing leads to a faster turnaround and less human error.

Helping the team leave behind tasks that are often repetitive and time-consuming by nature makes room for strategic tasks. These can be tasks that actually add value to the business. Efficiencies can then result in greater savings for the organisation. Especially when it comes to the utilisation of resources.

12.4 Benefits of E-invoicing

By doing away with paper invoices and manual processing, you can save a lot of money and time. The advantages lie in the level of connection you can establish. You'll make these connections between your invoicing software and other business systems. It will also help with connecting to trading partners.

Incorporating e-invoices into the AP automation solution further promotes touchless invoice processing. This is especially true for accounts payable. This helps free up time and resources for more important and value-adding duties.

The cost savings for businesses are unquestionably the biggest benefit of digitising invoicing. Invoicing by hand is difficult, expensive, and time-consuming. Companies can save up to 80% by switching from paper invoices to electronic invoicing.

You save money on supplies, printing, and shipping by using a digital outbound invoice. Additionally, you can make personnel capacity savings. You'll deliver invoices faster, and you can reduce manual sources of error. You'll also make payments faster using e-invoicing, thus increasing liquidity.

A good initial step in your company's digital transformation path can be starting to send and receive e-invoices. This can also be a crucial step in ensuring that your business processes are effective and scalable to accommodate future growth.

12.5 What's the difference between an invoice and an e-invoice?

An e-invoice is *not* the same as a paper invoice that's been uploaded into a digital format like a PDF. As digital files, e-invoices contain structured data designed to be automatically exchanged and processed by accounting and ERP systems.

It's the structured data that differentiates an e-invoice from a PDF or digitally transmitted scanned paper invoice.

12.6 How does e-invoicing work?

E-invoices typically use one of many structured data formats, which control how the invoice can be sent, viewed, and accepted. In general, there are two groups:

- A 'pure' **structured e-invoice format** for electronic data interchange (EDI) is machine readable but cannot be read by humans
- A **hybrid e-invoice format** contains structured data readable by machines *and* a visual format that can be read by humans

12.7 How do I send an e-invoice?

Electronic invoices can be sent through an open network like Peppol (Pan-European Public Procurement Online), via a government portal or private EDI connection, or via a service provider such as Avalara. Note that customers must be able to receive e-invoices, so typically you cannot send an e-invoice without first communicating with your customers. Everyone will have to be on board, so it's best to start the conversation early.

When you send an e-invoice, structured data such as ANSI X12, CSV, EDIFACT, XML, VDA or another machine-readable format is transferred directly into the buyer's accounting or ERP system.

12.8 When is e-invoicing required?

A growing number of countries require the use of e-invoices for business-to-government (B2G) or business-to-business (B2B) transactions. This process automation can lead to great savings and, in many cases, give tax authorities detailed insight into business transactions.

Where there are e-invoicing mandates for business-to-consumer (B2C) transactions, live reporting of issued invoices is also required because consumers cannot read structured data.

Many countries that don't already have e-invoicing or live reporting mandates are moving in that direction. "E-invoicing is the clear direction of travel for governments and tax authorities around the globe," notes Alex Baulf, Senior Director of Global Indirect Tax at Avalara.

Some jurisdictions take the post-audit model, meaning the e-invoice is sent to tax authorities only after the transaction has been completed.

In other jurisdictions, the tax authority sits in between the seller and the buyer. "Businesses are being forced to submit transaction-level details directly to the tax authority, in close to real time or real time."

The principal reason for this shift to mandatory use of electronic invoicing is to improve tax compliance. The European Union has a staggering value-added tax (VAT) gap — the difference between the expected and actual VAT collections.

12.9 E-invoicing can help close the VAT gap

E-invoicing helps reduce tax errors as well as tax fraud by giving tax authorities visibility into transactional tax data. In some countries, including Brazil and Italy, the tax authority must approve all e-invoices before they can be transmitted to the customer, or get directly involved in the invoicing process and issue the final invoices itself. Such real-time reporting cannot be achieved without e-invoicing.

The European Commission considers e-invoicing critical to fighting VAT fraud and reducing administrative and compliance costs for businesses. Because of how government is structured in the U.S., and because the U.S. doesn't suffer from the same degree of sales tax fraud, there are no e-invoicing mandates in the U.S. at this time.

However, the Federal Reserve and the Business Payments Coalition launched an e-invoicing exchange market pilot program in September 2021; the resulting electronic exchange network, now overseen by the Digital Business Networks Alliance, allows businesses to securely share electronic supply chain documents with one another.

12.10 How can e-invoicing impact my business?

E-invoicing can greatly increase efficiency in your finance departments by automating the invoicing process end to end.

In addition, you may not be able to do business in certain countries if your business doesn't have the ability to issue and/or receive electronic invoices. The more jurisdictions implement e-invoicing mandates, the more you'll feel constrained unless you can comply with them. This list of new and proposed e-invoicing requirements by country shows what you're up against.

Government mandates aside, there are benefits to implementing electronic invoices.

12.11 What are the benefits of e-invoicing for my business?

E-invoicing can:

- Accelerate invoice payment by reducing lag time
- Decrease administrative delays
- Enhance security due to encrypted file transfer, digital signatures, and secure networks
- Improve efficiency by streamlining AP/AR processes
- Lessen manual work, decrease human errors, and improve invoice data accuracy
- Promote transparency
- Reduce costs associated with printing, posting, processing, and archiving paper invoices

12.12 How can e-invoicing improve my cash flow?

E-invoicing can improve your cash flow by shrinking the lag between billing and payment. Electronic invoices won't be sent to the wrong person or get lost in the mail. On the other side of the transaction, businesses that receive e-invoices save on processing and handling because they save human work.

Businesses that implement e-invoicing may also be able to spend less on labor and supplies. According to a report by Billentis, automated e-invoicing can result in cost savings of 60–80%, as compared to conventional paper invoice processing.

12.13 How do I transition to e-invoicing?

Switching to an e-invoicing system requires planning. It's important to consider your current invoicing as well as your future invoicing needs (e.g., invoice volume and customer location) so you implement a system that can handle existing and anticipated regulatory requirements. This is complicated by ever-evolving (and multiplying) e-invoicing mandates.

E-Invoicing phases Electronic Invoicing is composed of two main phases, as follows:

1. Phase 1 (Generation Phase): Generation of Electronic Invoices Phase, where Persons subject to the E-Invoicing Regulations must generate Electronic Invoices and associated Electronic Notes in accordance with the clauses set forth under the Resolution on the E-INVOICING BYLAW and The Controls, Requirements, Technical Specifications And Procedural Rules For Implementing The Provisions Of The E-Invoicing Regulation and any subsequent resolutions. This phase has been implemented effectively by 4th of December 2021.

2. Phase 2 (Integration Phase): Integration Phase, where Persons subject to the E-Invoicing Regulations must integrate their systems with the Authority's system (FATOORA) in accordance with the clauses set forth under the Resolution on the Controls, Requirements, Technical Specifications and Procedural Rules and any subsequent resolutions. The second phase (integration phase) shall be implemented starting from 1st of January 2023 onwards. The second phase (integration phase) will be implemented in groups and will be mandated to Persons subject to the E-Invoicing Regulations based on the criteria set by the Authority. Notifications to the target groups will be initiated at least six months in advance

12.14 Guidelines of Electronic Invoicing

12.14.1 Electronic Invoicing

It is a mechanism that aims to transform the process of issuing paper invoices and notes into an electronic process that allows the exchange of invoices and debit and credit notes and their processing in a structured electronic format organized between the seller and the buyer.

12.14.2 Tax Invoice

A Tax Invoice as per Article 53(1) of VAT Implementing Regulations that is generated and stored in a structured electronic format through electronic means. Standard Tax Invoices are generally issued in Business to Business (B2B) transactions. A paper invoice that is converted into an electronic format through copying, scanning, or any other method is not considered an electronic invoice.

12.14.3 Simplified Tax Invoice:

A Simplified Tax Invoice as per Article 53(7) of VAT Implementing Regulations that is generated and stored in a structured electronic format generally issued for a B2C (business to consumer) transaction and does not generally include the buyer's details1. Optionally, Simplified Tax Invoices may also be issued for business-to-business transactions in case the value of supply is below SAR 1,000.

12.14.4 . Electronic Note:

Debit and credit notes that must be issued in accordance with the Article 54 of VAT Implementing Regulation, and which are generated and stored in a structured electronic format through electronic means. Paper notes that are converted into electronic format through copying, scanning, or any other method, are not considered electronic notes for the purposes of this Regulation.

12.14.5 Debit Note

Debit notes are issued by the sellers in order to issue a correction in value to buyers. Debit notes are used for increasing the value of the original invoice or the VAT amount. Debit notes follow the same format as the invoice for which they have been issued.

12.14.6. Credit Note

Credit notes are issued by the sellers in order to refund buyers and are used to correct invoices information if generated with an error. Credit notes follow the same format as the invoice they have been issued upon.

12.14.7. E-Invoice Solution

The compliant solution which is used for generating Electronic Invoices and Electronic Notes. Such a solution must fulfil the specifications and requirements set forth under the resolution on the Controls, Requirements, Technical Specifications and Procedural Rules for Implementing the Provisions of the E-Invoicing Regulation. An E-Invoice Solution may contain one or more Units.

12.14.8. FATOORA Portal

ZATCA's portal through which Tax Invoice, Simplified Tax Invoice, and electronic credit/ debit note data is received, which are generated by the E-Invoice Solutions used by Persons subject to the E-Invoicing Regulations. This portal aims to onboard the user's EGS Unit through generating cryptographic stamp identifier or renewing the existing one or revoking it. In addition, the user can view the list of onboarded solutions and devices.

12.14.9. Cryptographic Stamp

An electronic stamp which is created via cryptographic algorithms to ensure authenticity of origin and integrity of content of the data for the Electronic Invoices and its associated Electronic Notes, and to ensure the identity verification of the issuer for the Invoices and Notes for the purpose of ensuring compliance with the provisions and controls of the VAT Law and its Implementing Regulation regarding the generation of Electronic Invoices and Notes. For technical details, please refer to the Security Features Implementation Standard.

12.14.10. Cryptographic Stamp Identifier (CSID):

A Cryptographic Stamp Identifier (CSID) is a unique identifier that links the E-Invoice Solution Unit and a trusted third party able to confirm the identity of the Person subject to the E-Invoicing Regulation and uniquely identify their unit. For technical details, please refer to the Security Features Implementation Standard.

12.14.11 UUID:

A 128-bit number, generated by an algorithm chosen to make it unlikely that the same identifier will be generated by anyone else in the known universe using the same algorithm. The UUID is generated by a compliant E-Invoice Solution and stored inside the XML invoice. Note: In Windows OS UUIDs are referred to by the term GUID.

12.15. FATOORA Portal:

ZATCA's portal through which Tax Invoice, Simplified Tax Invoice, and electronic credit/ debit note data is received, which are generated by the E-Invoice Solutions used by Persons subject to the E-Invoicing Regulations. This portal aims to onboard the user's EGS Unit through generating cryptographic stamp identifier or renewing the existing one or revoking it. In addition, the user can view the list of onboarded solutions and devices.

12.16. Cryptographic Stamp:

An electronic stamp which is created via cryptographic algorithms to ensure authenticity of origin and integrity of content of the data for the Electronic Invoices and its associated Electronic Notes, and to ensure the identity verification of the issuer for the Invoices and Notes for the purpose of ensuring compliance with the provisions and controls of the VAT Law and its Implementing Regulation regarding the generation of Electronic Invoices and Notes. For technical details, please refer to the Security Features Implementation Standard.

12.17. Clearance:

Clearance is the process where the Authority shall verify that the Electronic Tax Invoices and their associated Electronic Notes transmitted to it (through integration) by the persons subject to E-Invoicing Regulation, fulfil the controls and details specified in the E-Invoicing Resolution, Annexes (1) and (2) of the Resolution, and the relevant technical documentation. The Authority shall insert the Cryptographic Stamp only on the Invoices and Notes which fulfil the aforementioned controls and details. Please note that the process of Clearance is not applicable to Simplified Tax Invoices.

12.18. Reporting of Simplified Tax Invoices and their associated notes:

Reporting is the process of sharing of the Simplified Tax Invoices and their associated Notes which are generated electronically - which include the Cryptographic Stamp as specified in Clause (Fourth) of the E-Invoicing Resolution- with the Authority by the persons subject to E-Invoicing Regulation. Persons subject to the E-Invoicing Regulation will be required to transmit all Simplified Tax Invoices to the FATOORA Portal within (24) hours from its issuance.

12.19. Human Readable Format:

The human readable format of the invoice is a recognizable invoice that can be read and understood by a human reader (including buyers and the Authority).

12.20. The Authority's Toolkit:

The Authority toolkit is the testing toolkits provided by the Authority to allow Persons subject to the E-Invoicing Regulation to verify that their solutions generate compliant invoices and can be validated by the FATOORA Portal after integration. There are three tools provided the sandbox, SDK and web-based validator, for more details please check the sandbox webpage.

12.21 Types of E-Invoices

12.21.1. Tax Invoices for Phase 1 (Generation Phase)

a. A Tax invoice is an invoice issued for most B2B and B2G transactions with fields defined in Article 53 (5), VAT Implementing Regulations and Annex 2 of E Invoicing Resolution. The fields required for Generation Phase and Integration Phase to be included within the Tax Invoice are included in the Annex 2 of the E-Invoicing Resolution.

b. For Phase 1 (Generation Phase), the taxpayer must generate a Tax Invoice including additional data fields prescribed in the Annex 2 of E-Invoicing Resolution in an electronic format using a compliant E-Invoice Generation Solution (EGS). There is no specific format prescribed for Phase 1 Tax Invoices (such as XML format or PDF/A-3 format). Taxpayers can generate it in any electronic format, however, a paper invoice that is converted into an electronic format through copying, scanning, or any other method is not considered a compliant E-Invoice.

c. Also, for the Phase 1 (Generation Phase) invoices, there is no specific format prescribed for sharing / presentment to the buyers. Phase 1 invoices can be presented in the any electronic format.

12.21.2. Tax Invoices for Phase 2 (Integration Phase)

a. For Phase 2 (Integration Phase), the taxpayer must generate a Tax Invoice including additional data fields prescribed in the Annex 2 of E-Invoicing Resolution in an electronic format using a compliant E-Invoice Generation Solution (EGS) which is Onboarded (click here for detailed technical guideline which defines the onboarding process). Phase 2 (Integration Phase) Tax Invoices must be generated in XML format or a PDF/A-3 (with embedded XML).

b. Phase 2 (Integration Phase) Tax Invoices must be submitted in XML format (not PDF/A-3) to FATOORA Platform for “Clearance” using APIs. FATOORA Platform will validate whether the Tax Invoice is compliant with XML Implementation Standard and run additional referential checks. Once the Tax Invoice pass validation checks, FATOORA Platform will “Clear” the Tax Invoice by including a Cryptographic Stamp and a QR Code to the XML. The “Cleared” XML will be sent back to the taxpayer using APIs. Further details are provided in Section 7 of this guideline.

c. Phase 2 (Integration Phase) invoices must be shared / presentment to the buyers in XML or PDF/A-3 (with embedded XML) format. Tax Invoices contain fields as per VAT legislations including the seller and buyer information, transaction and goods/services details in addition to other technical fields that are to be generated by the electronic invoicing solution. Sample images of the human readable format of the Tax Invoice are included in Section 4.6 of this guideline. Samples must be different for Phase 1 and Phase 2.

12.21.3. Simplified Tax Invoice

a. A Simplified Tax invoice is an invoice issued mostly for B2C transactions with fields defined in Article 53 (8), VAT Implementing Regulations and Annex 2 of E Invoicing Resolution. The fields required for Generation Phase and Integration Phase to be included within the Simplified Tax Invoice are included in the Annex 2 of the E-Invoicing Resolution.

b. Also, taxpayers have an option to generate Simplified Tax Invoices for the B2B transaction if the value of Taxable Supplies is less than 1,000 SAR. It must be noted that for

Simplified Invoices for B2C transaction can be generated for any value (even for transactions where value of Taxable Supplies exceed 1,000 SAR). This limit of 1,000 SAR is only applicable when the supplier chooses to issue Simplified Tax Invoice for B2B transactions.

c. For Phase 1 (Generation Phase), the taxpayer must generate a Simplified Tax Invoice including additional data fields prescribed in the Annex 2 of E-Invoicing Resolution electronically using a compliant E-Invoice Generation Solution (EGS). There is no specific format prescribed for Phase 1 Simplified Tax Invoices (such as XML format or PDF/A-3 format). Taxpayers can generate it in any electronic format, however, a paper invoice that is converted into an electronic format through copying, scanning, or any other method is not considered a compliant E-Invoice generated electronically.

d. Simplified Tax Invoices that has been generated electronically must be shared / presented to the buyers in a printed copy. Alternatively, such Simplified Tax Invoice or its associated Notes - upon the agreement between the transaction parties - may also be shared with customers in its electronic format or any other human readable format with customers

12.21.4. Simplified Tax Invoices for Phase 2 (Integration Phase)

a. The taxpayer must generate Simplified Tax Invoice including additional data fields prescribed in the Annex 2 of E-Invoicing Resolution in an electronic format using a compliant E-Invoice Generation Solution (EGS) which is Onboarded. Simplified Tax Invoices must be generated in XML format or a PDF/A-3 (with embedded XML). Taxpayer's EGS solution must stamp the XML using CSID issued by ZATCA and also include a QR Code which is compliant with Phase 2 requirements (9 tags in TLV base64 format).

B. Once a compliant Simplified Tax Invoice is generated (after stamping and applying QR code), it must be shared / presented to the buyer immediately in a printed copy. Alternatively, such Simplified Tax Invoice or its associated Notes - upon the agreement between the transaction parties - may also be shared with customers in its electronic format or any other human readable format with customers.

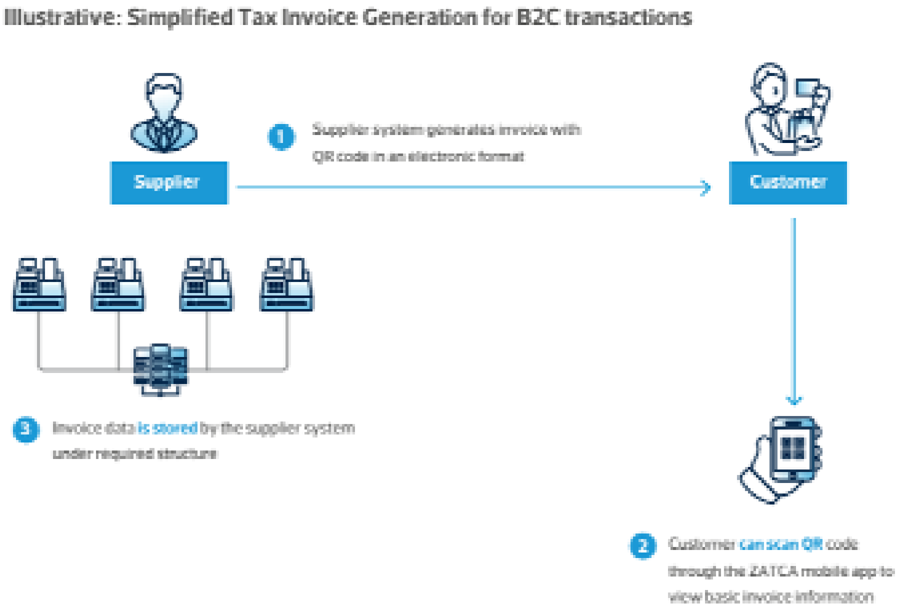
c. Taxpayers must submit the Simplified Tax Invoices in XML format (not PDF/A-3) to FATOORA Platform for "Reporting" within 24 hours of generation using APIs. FATOORA Platform will validate whether the Tax Invoice is compliant with XML Implementation Standard and run additional referential checks. Once the Simplified Tax Invoice pass validation checks, FATOORA Platform will provide an API response.

Credit and Debit Notes Electronic Credit / Debit notes are issued for a Tax Invoices / Simplified Tax Invoices (after an e- invoice has been issued), wherein the transaction is adjusted subject to Article 40 (1) and Article 54(3) of VAT Implementing Regulations.

Credit and Debit notes must be issued with a reference to the original invoice(s) to which they are issued. The reference fields can be used to indicate the Invoice Reference Number(s) of Original Invoice(s) to which Credit Note pertains. In case, a single Credit Note relates to multiple Original Invoices, then taxpayers can provide Invoice Reference Numbers as a range (for example IRN from 001 to IRN 100 issued during the period 1 Jan 2022 to 31 March 2022). The type of credit/debit note follows the type of invoice that they are issued against.

12.22 Sample visual examples of E- invoices

Each type of E-Invoice and associated note may be presented in human readable form. The fields required to be visible on such a representation are indicated in the E-Invoicing Resolution in Annex (2). This section contains examples of fully compliant visualized E-Invoices that contain the fields required starting 1st January 2023 (in waves by targeted taxpayer groups).


Illustrative: Simplified Tax Invoice Generation for B2C transactions
Supplier
1 Supplier system generates invoice with QR code in an electronic format
Customer
3 Invoice data is stored by the supplier system under required structure
2 Customer can scan QR code through the ZATCA mobile app to view basic invoice information

12.23 Technical Requirements

● All E-Invoice Solutions must be able to connect to the internet in order to share invoices with the Authority.

● The E-Invoice Solutions must be able to connect with an API published by the Authority in order to share invoices. Specific integration requirements are published on the Authority's website, and E-Invoice Solution vendors will have enough time to update their products and services.

● The E-Invoice Solutions must have tamper-proofing mechanisms that prevent any modification or tampering with invoices or the solution itself, and must be able to record and detect any tampering attempts.

● Persons subject to the E-Invoicing Regulation must ensure that their Compliant E-Invoice Solutions must be tamper-resistant and include a mechanism which prevents tampering and reveals tampering attempts that might occur.

1. These solutions contain functionalities that prohibit users from directly changing the solution and invoice generation.

2. The anti-tampering mechanisms include: Prevention of invoice counter reset: Resetting the invoice counter should not be a function available in an E-Invoice Solution and access to the counter value should be protected from system users.

Prevention of date changes: Resetting the system date should be inaccessible to system users.

Prevention of deletion or modification of invoices: Users of the E-Invoice Solution should not have the ability to delete or change E-Invoice and associated Note XML documents stored on by the solution. The solution should be equipped with sufficient memory to store the E-Invoice and associated Note XML documents generated by it.

Prevention of uncontrolled access: Access to E-Invoice Solution functions must always be via a logged in user who is granted access only to functions that are necessary to perform their role

As per VAT Implementing Regulations, if the data is hosted on the cloud, it must be accessible through a direct link that can be made available to the Authority. This requirement is mandatory for audit purposes as per VAT Implementing Regulations

12.24 Summary

The system must allow Persons subject to the E-Invoicing Regulation to export and save their invoices onto an external archival system

Each stored invoice must follow a naming convention for naming of the file: VAT Registration (tax registration number) + Timestamp (date and time at the point of invoice generation) + Invoice Reference Number

Taxpayer's E-Invoice Solutions may reside on the cloud in accordance with VAT Implementing Regulation, however additional non-tax-related regulations may apply to the taxpayer entity, such as National Cybersecurity Authority published laws and any other applicable regulations or controls

12.25 Key words

E-invoicing makes use of a variety of tech and entry methods. It is often used as a catch-all word to denote any approach to presenting an electronic invoice to a client for payment

A 'pure' structured e-invoice format for electronic data interchange (EDI) is machine readable but cannot be read by humans

A **hybrid e-invoice format** contains structured data readable by machines *and* a visual format that can be read by humans

Debit Note- Debit notes are issued by the sellers in order to issue a correction in value to buyers. Debit notes are used for increasing the value of the original invoice or the VAT amount. Debit notes follow the same format as the invoice for which they have been issued.

Credit Note- Credit notes are issued by the sellers in order to refund buyers and are used to correct invoices information if generated with an error. Credit notes follow the same format as the invoice they have been issued upon.

Cryptographic Stamp Identifier (CSID)- A Cryptographic Stamp Identifier (CSID) is a unique identifier that links the E-Invoice Solution Unit and a trusted third party able to confirm the identity of the Person subject to the E-Invoicing Regulation and uniquely identify their unit. For technical details, please refer to the Security Features Implementation Standard

12.26 Self Assessment Questions

1.Discuss the E-invoicing Work

2.Describe the Benefits of E-invoicing work

3. Briefly Explain the difference between an invoice and an e-invoice

4.Examine the Guidelines of the Electronic Invoicing

12.27 Suggested Readings

1. Engel-Flechsig, S. 2001. Securing the new global economy, Mobile Commerce World.

2. Pandey, S. (2013, April 23). Airtel Money. (G. S. Sambhy, Interviewer) Mumbai, Maharastra, India.

3. Tiwari, R., and Buse, S. 2007. The Mobile Commerce Prospects: A strategic analysis of opportunities in the banking sector (PDF).

Dr.Ch.Prasad