Course	ETC: Introduction to Cybersecurity
BRANCH	Computer Science and engineering

Done By:	Dr Krishnappa H K
	Associate Professor

VARIOUS TYPES OF DIGITAL PAYMENT SYSTEMS

- *Banking Cards (Debit/Credit/Cash/ Travel/Others) and Mobile Wallets.*
- *Point of Sale.*
- *Internet Banking.*
- *Mobile Banking.*
- *Banks Pre-Paid Cards.*
- *Prepaid Payment Instrument (PPI).*
- *Unstructured Supplementary Service Data (USSD).*
- *Aadhaar Enabled Payment System (AEPS).*
- *Unified Payments Interface (UPI).*
- *Micro ATMs.*
- *Bharat QR Code.*
- *Bharat Interface for Money (BHIM) App.*
- *Bharat Bill Payment System (BBPS).*

Digital Payment Systems : Introduction

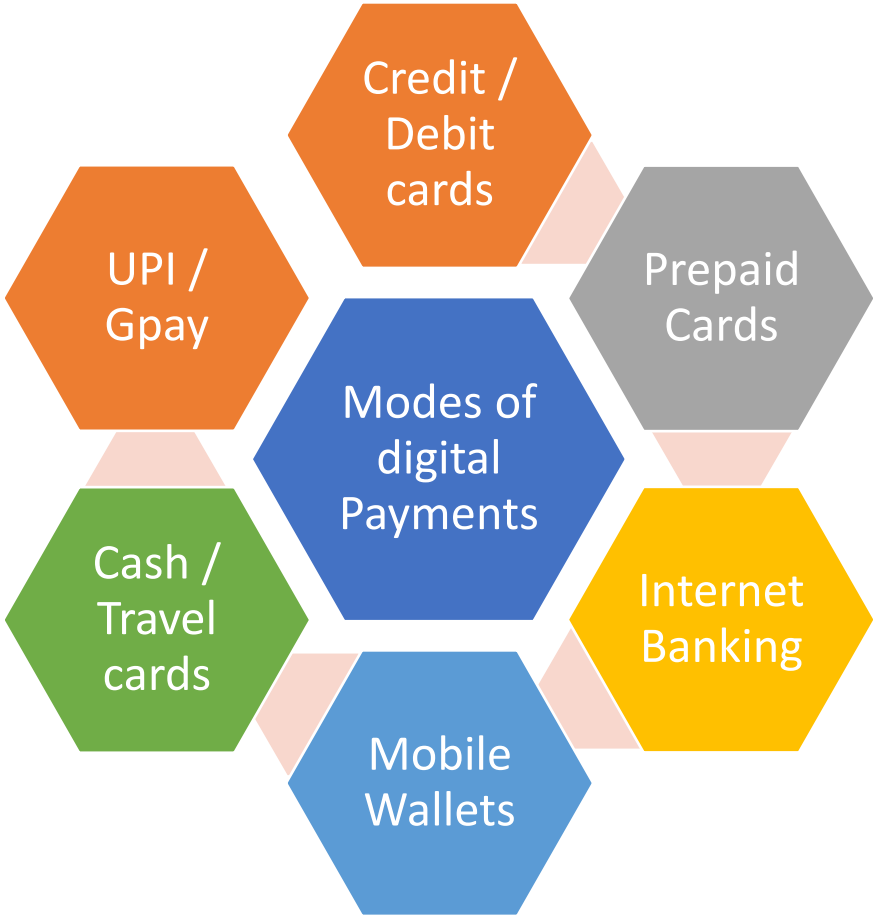
- Modern and convenient method of conducting financial transactions electronically.
- Allows transfer of money through digital channels, such as the internet or mobile devices, without the need for physical cash
- Significant growth and adoption in recent years, driven by technological advancements, increased internet penetration, and the widespread use of smartphones.

Digital v/s Cash transactions

	Digital	Cash	
Speed	✓	×	Digital payments provide convenience and speed against cash for carrying out transaction
Convenience	✓	×	Carrying physical cash can be inconvenient and pose a risk of theft or loss
Security	✓	×	Digital payments offer security measures through encryption and authentication
Universal Accessibility	×	✓	Cash transactions offer universal accessibility without relying on technology or internet connectivity
Traceability	✓	×	Cash payment lacks the traceability and security

The choice between digital payments and cash transactions depends upon individual preferences, technological access, and the level of security and convenience required in a particular situation.

Modes of digital Payments



Credit & Debit Cards

- Debit and credit cards have become indispensable tools in the modern world, revolutionizing the way people handle their finances.
- Debit cards allow to instantly deduct funds from the account and provide real-time financial awareness and help users stay within their budget.
- Credit cards allow users to borrow money up to a pre-approved credit limit.
- Responsible use of credit cards can help build a positive credit history and unlock various rewards and benefits.
- Both offer convenience, security, and financial management capabilities, making them essential companions in our cashless transactions-driven society.

Cash & Travel Cards

- Cash and travel cards are prepaid cards that have gained popularity as convenient and secure payment options for various purposes.
- Travel cards allow users to load foreign currencies onto the card before embarking on their trips.
- Both cash and travel cards offer the convenience of electronic payments without the need for a traditional bank account.
- These prepaid cards allow simplicity, security, and financial flexibility in daily lives and international adventures.

Prepaid Cards

- Prepaid cards are reloadable payment cards that are not linked to a bank account like Metro Cards, Gaming Cards etc.
- The amount is deducted from the card's balance when users make purchases using a prepaid card
- Prepaid gift cards are generally non-reloadable designed for gifting purposes.
- Unlike credit cards, prepaid cards do not require a credit check during the application process.

Mobile Wallets

- Mobile wallets have revolutionized the way financial transactions are conducted in the digital age.
- Serve as virtual repositories for various payment methods, loyalty cards, and financial assets and are accessible through smartphones and tablets.
- By digitization of credit and debit cards, mobile wallets provide users a seamless and secure experience for making purchases, both in-store and online.
- Mobile wallets incorporate peer-to-peer transfer functionalities, bill payment services, and loyalty program integration
- With increasing popularity, digital wallets are reshaping the way we interact with money and paving the way towards a cashless and interconnected financial landscape.

Popular Mobile Wallets in India

- Paytm is one of the most widely used mobile wallets in India. It started as a digital wallet but later expanded into a full-fledged payment platform offering bill payments, online shopping, ticket booking, and more.
- Google Pay (formerly Tez), also known as GPay, gained immense popularity for its simplicity and seamless integration with banks. It allows users to make payments using UPI (Unified Payments Interface) and send money to contacts instantly.
- PhonePe, acquired by Flipkart, became popular for its user-friendly interface and quick UPI-based transactions. It offered various services, including bill payments, recharges, and money transfers.
- Mobiwik, Amazon Pay and BHIM (Bharat Interface for Money - a government-backed UPI app) are other popular Mobile wallets

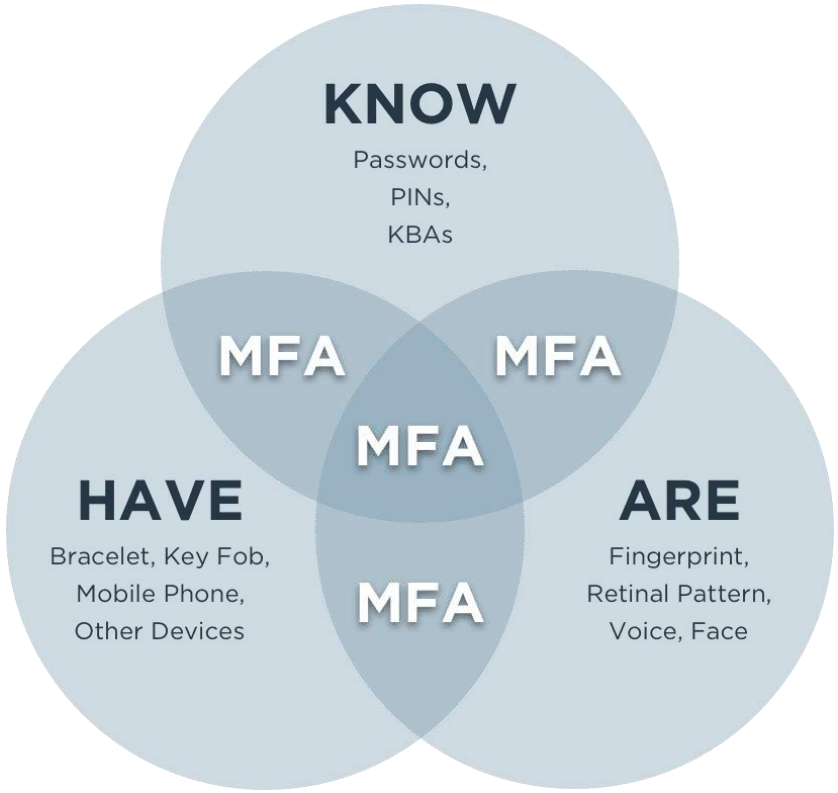
Security Measures in digital payments

- Advanced security technologies are used in both banking cards and mobile wallets to safeguard user information and protect against unauthorized access.
- EMV (Europay, Mastercard, Visa) Chip Technology
  - Banking Cards: Most modern banking cards are equipped with EMV chips. These small, embedded microchips generate a unique code for each transaction, making it difficult for fraudsters to clone the card. Unlike magnetic stripe cards, EMV chips provide an additional layer of security against card skimming and counterfeit fraud.
  - Mobile Wallets: When using mobile wallets for in-store purchases, the same EMV chip technology used in banking cards is emulated through Near Field Communication (NFC). This process ensures secure transactions between the mobile device and the payment terminal.

Security Measures in digital payments

- Biometrics
  - Banking Cards: Some newer banking cards come with biometric authentication features, such as fingerprint sensors. Cardholders can use their fingerprint to authorize transactions, adding an extra layer of security beyond the traditional PIN.
  - Mobile Wallets: Mobile wallets often incorporate biometric authentication methods like fingerprint scanning or facial recognition. Users need to authenticate themselves using their biometric data before they can access the wallet or complete a transaction.

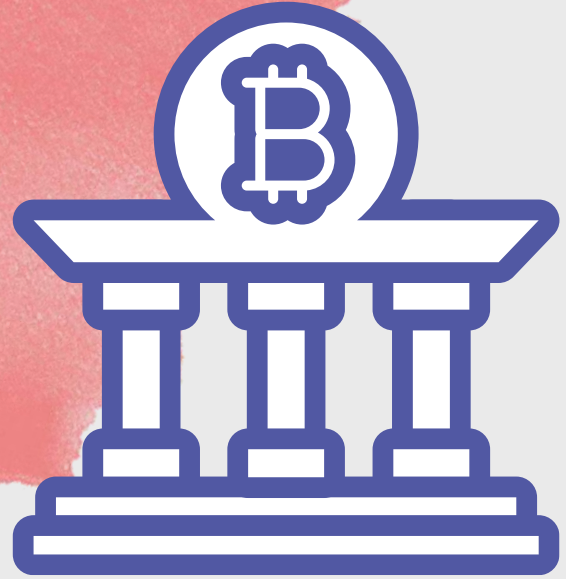
Security Measures in digital payments



- Multi-Factor Authentication (MFA)
  - Both Banking Cards and Mobile Wallets: Multi-factor authentication requires users to provide more than one form of verification before accessing the account or completing a transaction.
  - MFA typically combines something the user knows (e.g., PIN or password) with something the user has (e.g., physical card or smartphone) or something the user is (e.g., fingerprint or facial scan).

INTERNET BANKING

What is Internet Banking?



- Internet banking, also known as online banking or e-banking, is a service provided by banks and financial institutions that allows customers to conduct various banking transactions over the internet. It enables customers to manage their accounts, transfer funds, pay bills, and access other banking services using a web-based platform or mobile application.
- In simple terms, internet banking is a way for you to do your banking activities using the internet, just like you use your computer or smartphone to browse the web or use social media. Instead of going to a physical bank branch, you can access your bank account and perform various banking tasks online.
- With internet banking, you can check your account balance, view recent transactions, transfer money between your accounts, pay bills, and even apply for loans – all from the comfort of your own home or wherever you have an internet connection.
- It's like having a virtual bank branch at your fingertips, allowing you to manage your money and handle your finances conveniently and securely without having to visit a physical bank location. It's quick, easy, and available 24/7!
- first introduced by ICICI Bank in 1998.

Key features of Internet Banking

Account Management:

view their account balances, transaction history, and download account statements.

Fund Transfers:

transfer money between accounts held at other banks, domestically or internationally.

Bill Payments:

pay bills, such as utility bills, credit card bills, and other recurring payments, directly from their bank accounts

Mobile Banking:

Many banks offer mobile applications that allow customers to access internet banking services on their smartphones

Check Deposits:

banking platforms allow customers to deposit checks electronically using their smartphones.

Online Statements:

receive and view their account statements electronically, reducing the need for paper statements.

CYBERSECURITY IN INTERNET BANKING!

Common cybersecurity processes

Secure Login Processes

Data Encryption

Incident Response Plan

Secure Socket Layer (SSL) and Transport Layer Security (TLS)

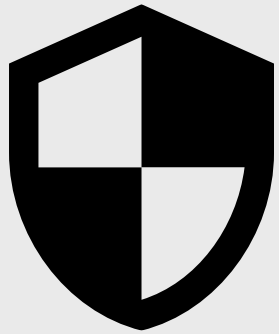
Firewalls

Two-Factor Authentication (2FA) and Multi-Factor Authentication (MFA)

Intrusion Detection and Prevention Systems (IDPS)

Continuous Monitoring and Auditing

Anti-Malware and Antivirus Software



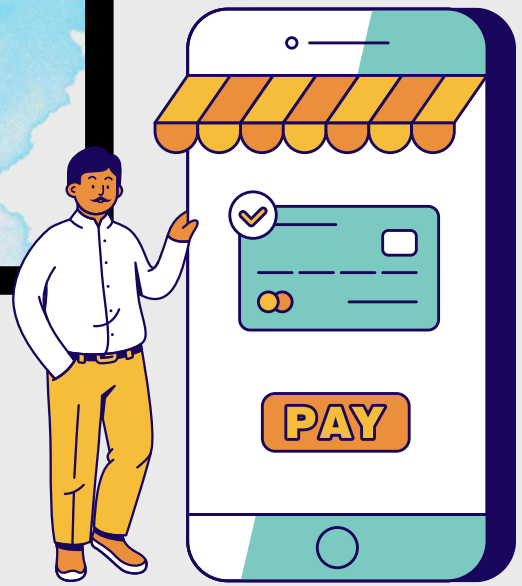
CASE STUDY!

The Indian government has reported 11,60,000 cyber-attacks in 2022. It is estimated to be three times more than in 2019. India has been the target of serious cyberattacks, such as the phishing attempt that nearly resulted in a $171 million fraudulent transaction in 2016 against the Union Bank of India.

PARAKALA: In a shocking incident, State Bank of India (SBI).Parakala branch manager was cheated by the cybercrime miscreants.Sakal Deo Singh working as manager in the SBl main branch of Parakala lost Rs 2.24,967 from his account. The incident came to light after he lodged a complaint with Parakala police. According to Sakal Deo Singh, he received a message from 8987861993 stating that "your BI account has been deactivated, pleass click on the link and update Pan card number immediately". He saw the message next morning and clicked on the link, immediately the SBl internet banking site was opened and he was asked enter the pass word. Soon after entering the password, he received a call from 7431829447 asking him that "we have sent an message and click on the same", the manager clicked on the message and entered password, updated Pan card, however it was not updated.

and he found that his money went missing.

POINT OF SALE!



What is point of sale?

A point of sale (POS) digital payment method refers to a payment system that allows customers to make transactions electronically at the point of sale, typically in physical retail locations. These methods enable customers to pay for goods and services using digital means, such as credit or debit cards, mobile wallets, contactless payments, or other electronic payment options.

1.Credit and Debit Cards: Customers can use their credit or debit cards, usually equipped with a magnetic stripe or an EMV chip, to make payments at the point of sale. The card's information is processed through a card reader or a terminal, and the transaction is authorized by the issuing bank.

2. Mobile Wallets: Mobile wallet apps, such as Apple Pay, Google Pay, Samsung Pay, or other similar platforms, allow customers to store their card information securely on their smartphones. They can then make payments by tapping their devices on compatible card readers.

3. Contactless Payments: Contactless payments use Near Field Communication (NFC) technology, enabling customers to pay for purchases by simply tapping or waving their contactless-enabled cards or smartphones near the POS terminal.

4. QR Code Payments: Some payment methods involve scanning QR codes displayed on the merchant's terminal with a smartphone camera. The customer's payment information is then processed via the associated app.

5. Mobile Banking Apps: Certain banking apps offer a feature that generates a one-time barcode or token that can be scanned at the POS terminal to complete the transaction.

6. Digital Wallets: In addition to mobile wallets, some platforms offer digital wallets specifically for in-store payments. These wallets might require a separate app or account setup.

7. Wearable Devices: Some payment methods allow customers to make payments using wearable devices like smartwatches or fitness trackers equipped with NFC technology.

TYPES OF CYBERSECURITY USED

Biometric Authentication

Mobile wallets often use biometric authentication methods, such as fingerprint recognition Biometric data is unique to each individual, making it difficult for unauthorized users to access the mobile wallet.

Device Authentication

Mobile wallets may employ device-level authentication, checking the integrity and security features of the user's mobile device before allowing access to the stored payment information.

As an added security measure, mobile wallets may require 2FA, such as a one-time password (OTP) or biometric verification, to authorize transactions or access the app.

Two-Factor Authentication (2FA)

Mobile wallets often provide real-time transaction alerts to users, notifying them of any suspicious or unauthorized activity. This allows users to take immediate action if they notice any fraudulent transactions.

Transaction Alerts

TYPES OF CYBERSECURITY USED FOR CREDIT CARDS

EMV Chip Technology

EMV (Europay, Mastercard, Visa) chip technology, commonly known as "chip and PIN" or "chip and signature," provides enhanced security over traditional magnetic stripe cards. The microchip embedded in the card generates unique transaction data for each purchase, making it challenging for attackers to create counterfeit cards.

Secure Network Infrastructure

Financial institutions and payment processors invest in robust network security to safeguard cardholder data. This includes firewalls, intrusion detection systems (IDS), and other security measures to monitor and defend against unauthorized access attempts.

Sophisticated fraud detection systems that monitor transactions in real-time. These systems use machine learning algorithms to analyze transaction patterns and detect any suspicious activity, such as unusual spending behavior or transactions from unfamiliar locations.

Fraud Detection Systems

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards established to protect cardholder data during credit and debit card transactions. Merchants and payment processors are required to comply with PCI DSS to ensure the security of cardholder information.

PCI DSS Compliance

CASE STUDY

Shomiron Das Gupta, an intrusion analyst who has been building threat-detection systems for more than a decade and founder of DNIF (a platform that offers cyber-security solutions), told Hindustan Times, “In cases where cloned cards are used by fraudsters to withdraw money from ATMs, the banks can come up with the OTP system, where after swiping your card, an OTP request is received on your mobile and this OTP is mandatory to withdraw money. This way, even if the fraudster has your cloned card and PIN, he cannot withdraw money.”

Gupta added, “If this option is not possible, then another option to stop such frauds would be where the user can scan a unique QR code on the ATM. As soon as it is done, the user can withdraw cash. We can eliminate the use of cards or any contact with the ATM for that matter. We have technology to shift to a card-less economy.”

CASE STUDY

The increase in digital payments, especially after the Covid-19 lockdown, seems to have a correlation with the higher number of complaints.

Explaining how UP deceptions are perpetrated, a police officer said the scammer sends some money to the victim through UP and then makes a phone call claiming that the amount was sent by mistake. He then sends a link and requests the victim to click on the link to initiate the return of the money.When the person does so, he or she loses control of his digital wallet and bank account.Another officer said the fraudsters also use QR codes to dupe people. "The crook informs a potential target of money being transferred using a QR code. When the code is scanned by the victim, he or she is asked to enter the UP PIN. If the PIN is shared, the money, instead of being credited, is deducted from the user's account." the officer said. Prashant Gautam, DCP (IFS), cautioned that in most cases, fraudsters will ask the victim to enter a UPI to receive money.

Various types of Digital Payment Systems: Mobile Banking and Bank Pre-Paid Cards

Introduction

In today's world, technology has made it easier than ever to make payments online, but with that convenience comes the risk of cyber threats. Today, we will explore the various risks associated with mobile banking and bank pre-paid cards, as well as provide tips on how to protect yourself from these risks.

As we delve into these topics, keep in mind that cyber security is not just a concern for businesses or governments, but for individuals as well. We all have personal information that can be targeted by cyber criminals, so it's important to stay informed and take steps to protect ourselves.

What are digital payments?

Digital payments refer to the electronic transfer of money from one party to another. This can be done through various methods such as online banking, mobile payments, and e-wallets. With digital payments, there is no need for physical cash or checks, making transactions faster and more convenient.

Examples of digital payments include credit card payments, UPI (Unified Payments Interface)- (Eg: Paytm and Google Pay) and cryptocurrency transactions. These payment methods are becoming increasingly popular as more people turn to online shopping and mobile banking for their financial needs.

Mobile banking

Mobile banking is a digital payment method that allows users to access their bank accounts and conduct transactions through their mobile devices. With mobile banking, users can transfer funds, pay bills, and check their account balances on the go. The benefits of using mobile banking for digital payments include convenience, accessibility, and speed. However, there are also drawbacks to consider, such as potential security risks. It is important to be aware of these risks and take steps to protect oneself from cyber threats when using mobile banking.

Cyber security risks with mobile banking

Mobile banking has become increasingly popular in recent years, but it also comes with its fair share of cyber security risks.

One major risk is phishing attacks, where cyber criminals try to trick users into giving away sensitive information such as login credentials or personal data. These attacks can be difficult to spot, as they often appear to be legitimate emails or messages from the bank.

Cyber security risks with mobile banking

Another risk is malware, which can infect a user's device and steal sensitive information without their knowledge. This can happen through malicious apps or links that are clicked on while using mobile banking.

To protect oneself from these risks, it is important to always be vigilant when using mobile banking. Users should never click on suspicious links or provide personal information unless they are certain it is a legitimate request from the bank. It is also important to keep anti-virus software up to date and to use strong passwords to prevent unauthorized access.

Bank pre-paid cards

Bank pre-paid cards are a type of payment card that is loaded with funds in advance. They work like debit cards, but instead of being linked to a bank account, they are linked to a prepaid balance. This means that you can only spend the amount that has been loaded onto the card.

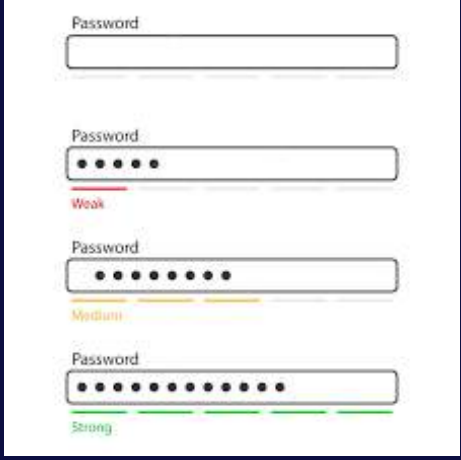
One of the benefits of using bank pre-paid cards for digital payments is that they can help you avoid overspending and going into debt. Since you can only spend what you have loaded onto the card, it can be a good way to stick to a budget. However, one drawback is that some cards come with fees, such as activation fees or monthly maintenance fees.

Cyber security risks with bank pre-paid cards

- Bank pre-paid cards are a convenient way to make digital payments, but they also come with their own set of cyber security risks. One of the biggest risks is unauthorized transactions, where someone gains access to your card information and uses it to make purchases without your knowledge or consent. Another risk is card skimming, where thieves use special devices to steal your card information when you use it to make a payment.
- To protect yourself from these risks, it's important to monitor your bank account regularly for any unauthorized transactions and report them immediately. You should also keep your card in a secure location and never share your card information with anyone. Additionally, consider using a virtual card number, which generates a unique number for each transaction and helps prevent fraud.

Best Cyber Security practises: Using strong passwords

- When it comes to digital payments, using strong passwords is essential for protecting your sensitive information from cyber criminals. A strong password should be at least 12 characters long and include a mix of upper and lowercase letters, numbers, and symbols. Avoid using common words or personal information that can be easily guessed.
- To manage your passwords securely, consider using a password manager tool that encrypts and stores your passwords in a safe location. This way, you only need to remember one strong master password instead of multiple passwords for different accounts. Additionally, enable two-factor authentication whenever possible for an extra layer of security.



New Password

Everyone else explaining cyber security

Weak

New Password

Krishnappa Sir explaining cyber security

Strong

Best Cyber Security practises: Keeping software up to date

Keeping your software up to date is crucial when it comes to digital payments. Software updates often include important security patches that address vulnerabilities and protect against cyber attacks.

To ensure that your software is always up to date, make sure to enable automatic updates whenever possible. You should also regularly check for updates manually, especially if you haven't used a particular app or program in a while.

Best Cyber Security practises:Avoiding public Wi-Fi

When it comes to making digital payments, using public Wi-Fi can be a major security risk. Hackers can easily intercept your data and steal sensitive information such as credit card numbers and login credentials. It's important to avoid using public Wi-Fi when making digital payments whenever possible.

If you must use public Wi-Fi, there are steps you can take to protect yourself. First, make sure you only connect to secure networks that require a password. Avoid using open networks that anyone can access. Second, use a virtual private network (VPN) to encrypt your data and protect your privacy. Finally, be cautious of any suspicious activity or pop-ups on your device while using public Wi-Fi.

Conclusion

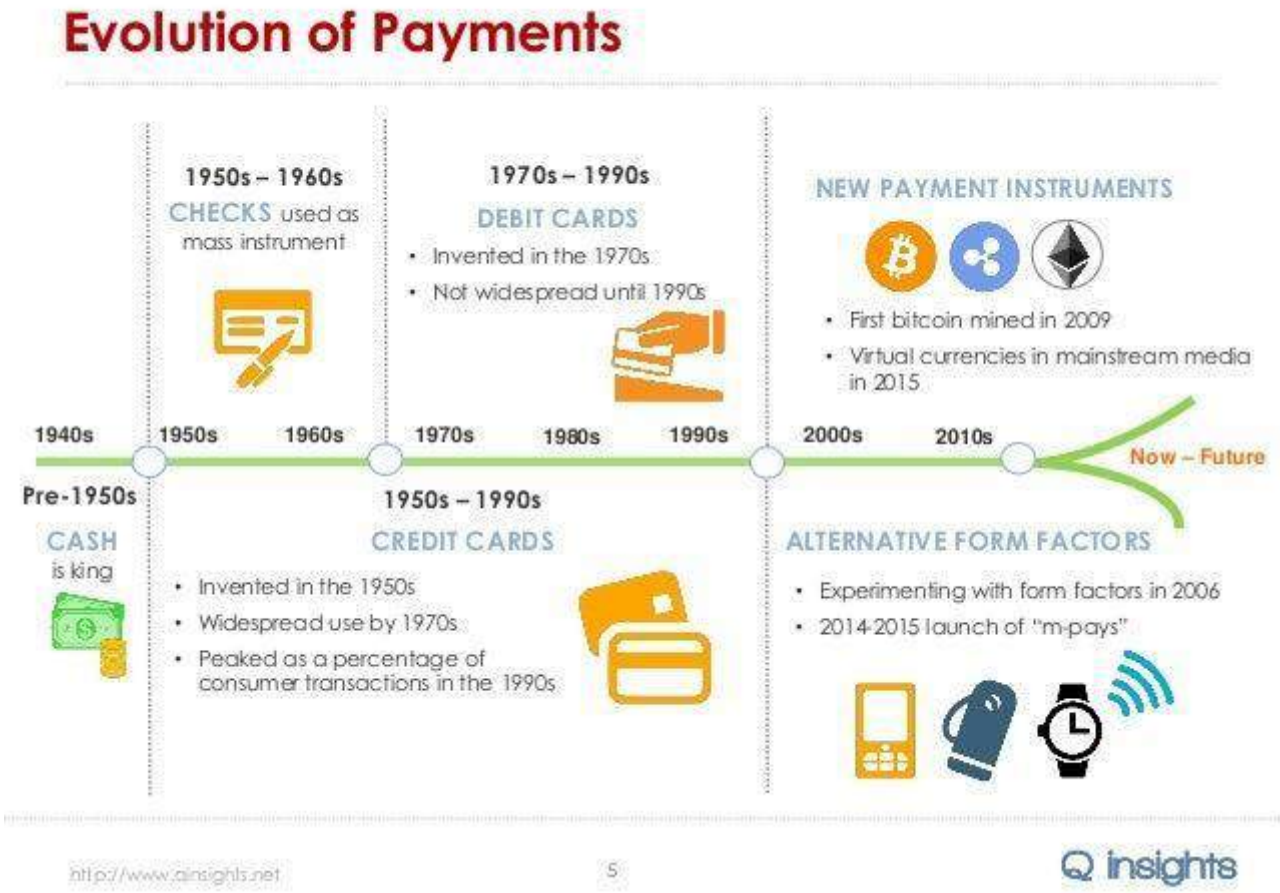
In conclusion, we have discussed the importance of cyber security when using digital payments, whether it be through mobile banking or bank pre-paid cards. We have explored the various cyber security risks associated with these payment methods and provided tips on how to protect oneself from these risks.

It is important to remember to follow cyber security best practices such as using strong passwords, keeping software up to date, and avoiding public Wi-Fi. By taking these steps, we can ensure that our digital payments are secure and protected from cyber threats.

Prepaid Payment Instrument (PPI) and Unstructured Supplementary Service Data (USSD)

- The Evolution of Digital Payment Systems
  - What are Prepaid Payment Instruments?
  - Types of Prepaid Payment Instruments
  - Advantages of Prepaid Payment Instruments
  - Disadvantages of Prepaid Payment Instruments
  - What is USSD?
  - How USSD is Used for Digital Payments
  - Advantages of USSD for Digital Payments
  - Disadvantages of USSD for Digital Payments
  - Prepaid Payment Instruments vs. USSD

- Security in Digital Payment Systems.
- Common Security Risks in Digital Payment Systems
- How to Protect Yourself When Using Digital Payment Systems
- Regulatory Framework for Digital Payment Systems
  - Global Trends in Digital Payment Systems
  - The Future of Digital Payment Systems
  - Case Study: Successful Implementation of Prepaid Payment Instruments
  - Case Study: Successful Implementation of USSD for Digital Payments
  - Best Practices for Implementing Digital Payment Systems
  - Common Challenges in Implementing Digital Payment Systems
  - How to Overcome Challenges When Implementing Digital Payment Systems
  - The Role of Digital Payment Systems in Financial Inclusion
  - The Impact of Digital Payment Systems on the Economy
  - The Importance of Collaboration in Digital Payment Systems


Evolution of Payments
1950s – 1960s
CHECKS used as mass instrument
1970s – 1990s
DEBIT CARDS
• Invented in the 1970s
• Not widespread until 1990s
NEW PAYMENT INSTRUMENTS
• First bitcoin mined in 2009
• Virtual currencies in mainstream media in 2015
1940s
1950s
1960s
1970s
1980s
1990s
2000s
2010s
Now – Future
Pre-1950s
CASH
is king
1950s – 1990s
CREDIT CARDS
• Invented in the 1950s
• Widespread use by 1970s
• Peaked as a percentage of consumer transactions in the 1990s
ALTERNATIVE FORM FACTORS
• Experimenting with form factors in 2006
• 2014-2015 launch of "m-pays"
http://www.qinsights.net
5
Q insights

- Digital payment systems have come a long way since their inception. From the early days of online banking to the rise of mobile payments, these systems have evolved to meet the changing needs of consumers and businesses alike.
- Today, digital payment systems are faster, more secure, and more convenient than ever before. They allow us to make purchases from anywhere in the world, at any time of day or night. And as technology continues to advance, we can expect these systems to become even more sophisticated and user-friendly.


DISRUPTIVE BUSINESS ENABLERS
PREPAID PAYMENT INSTRUMENTS (PPI)
M2P
BUY NOW

- Prepaid payment instruments are a type of digital payment system that allows users to load funds onto a card or account in advance, which can then be used to make purchases or payments. These instruments are often used as an alternative to traditional credit or debit cards and can be particularly useful for individuals who do not have access to these types of financial products.
- There are several different types of prepaid payment instruments, including e-wallets, prepaid cards, and mobile wallets. E-wallets are virtual accounts that can be accessed through a smartphone or computer, while prepaid cards are physical cards that can be loaded with funds and used at merchants that accept them. Mobile wallets are similar to e-wallets, but are specifically designed for use on mobile devices.

- Prepaid payment instruments are a type of digital payment system that allows users to load funds onto a card or account in advance, which can then be used to make purchases. There are several types of prepaid payment instruments, including e-wallets, prepaid cards, and mobile wallets.
- E-wallets are digital accounts that can be used to store funds and make payments online or through a mobile app. Examples of e-wallets include PayPal, Venmo, and Google Wallet. Prepaid cards are physical cards that can be loaded with funds and used to make purchases at merchants that accept the card's network, such as Visa or Mastercard. Mobile wallets are similar to e-wallets but are specifically designed for use on a mobile device, often using Near Field Communication (NFC) technology to enable contactless payments. Examples of mobile wallets include Apple Pay, Samsung Pay, and Google Pay.

- Prepaid payment instruments offer a range of advantages that make them an attractive option for consumers. One of the key benefits is convenience – these instruments allow users to make payments quickly and easily, without the need to carry cash or visit a physical bank branch. For example, a person can use a prepaid card to pay for groceries at a store or to buy movie tickets online. This saves time and effort, making it a popular choice for busy individuals.
- Another advantage of prepaid payment instruments is security. These instruments are designed to protect users against fraud and theft, with features such as PIN codes, encryption, and transaction monitoring. For instance, if a prepaid card is lost or stolen, the user can report it to the issuer and have it blocked, preventing unauthorized transactions. This gives users peace of mind and helps to build trust in the system.


BANK
1234 5678 1234 5678
CARD
PAY
PAYMENT
APPROVED


DISADVANTAGE

- While prepaid payment instruments offer many advantages, there are also some potential drawbacks to using them. One of the biggest disadvantages is the fees associated with these systems. Users may be charged fees for transactions, loading funds onto their accounts, or other activities. These fees can add up quickly and eat into the value of the prepaid instrument.
- Another disadvantage of prepaid payment instruments is that they may have limited acceptance. Not all merchants or service providers may accept these forms of payment, which can limit the usefulness of the instrument for some users. Finally, there is also a risk of loss or theft associated with these instruments. If a user loses their prepaid card or has it stolen, they may lose the funds loaded onto it.


USSD
*#

- USSD stands for Unstructured Supplementary Service Data and is a technology used to send text messages between a mobile phone and an application server. Unlike SMS, USSD messages don't require an internet connection and are sent through the GSM network.
- When you use USSD for digital payments, you typically start by dialing a short code on your phone (e.g. *123#). This sends a request to the application server, which responds with a menu of options that you can select by entering a number on your keypad. The server then processes your request and sends a response back to your phone as a USSD message.

USSD Payment System

Mode of Transaction

- One of the biggest advantages of using USSD for digital payments is its accessibility. Unlike other digital payment systems that require a smartphone or internet connection, USSD can be used on any mobile phone, including basic feature phones. This makes it an ideal solution for people who do not have access to smartphones or reliable internet connections.
- Another advantage of USSD is its affordability. Because it uses a simple text-based interface, USSD requires very little data to operate. This means that users can make digital payments without incurring high data charges or needing a large data plan. In addition, because USSD does not require any special hardware or software, there are no additional costs associated with using this technology.


DISADVANTAGE

- While USSD has several advantages for digital payments, there are also some potential drawbacks that users should be aware of. One of these is limited functionality - USSD is primarily used for basic transactions like balance inquiries and fund transfers, and may not support more complex features like bill payments or peer-to-peer transfers.
- Another disadvantage of USSD is security concerns. Because USSD messages are transmitted over the airwaves, they can potentially be intercepted by hackers or other malicious actors. Additionally, because USSD does not use encryption, sensitive information like PINs or passwords could be vulnerable to interception. Finally, there is also a risk of errors when using USSD for digital payments, as mistyping a code or entering incorrect information could result in funds being sent to the wrong recipient.

Prepaid Payment Instruments vs. USSD

- Prepaid payment instruments and USSD are two popular digital payment systems that serve different purposes. Prepaid payment instruments, such as e-wallets and prepaid cards, allow users to store money and make payments without the need for a bank account. USSD, on the other hand, is a mobile technology that allows users to access services through a simple menu-based system.
- One key difference between prepaid payment instruments and USSD is their level of accessibility. Prepaid payment instruments require users to have a smartphone or computer with internet access, while USSD can be used on any mobile phone, even those without internet access. Another difference is their functionality - prepaid payment instruments offer more features, such as the ability to withdraw cash from ATMs, while USSD is limited to basic transactions like balance checks and money transfers.

Security in Digital Payment Systems

Security in Digital Payment Systems

- Security is a top priority in digital payment systems. With the rise of online transactions, it's important for users to feel confident that their personal and financial information is protected. Fortunately, there are many measures in place to ensure the security of digital payment systems.
- One of the most common security measures is encryption. This involves encoding data so that it can only be accessed by authorized parties. Many digital payment systems also use multi-factor authentication, which requires users to provide multiple forms of identification before accessing their accounts. Additionally, some systems use biometric technology, such as fingerprint or facial recognition, to verify user identity. These measures help to prevent fraud and protect users' sensitive information.

Common Security Risks in Digital Payment Systems

Common Security Risks in Digital Payment Systems

- One of the most significant security risks in digital payment systems is fraud. Fraudsters can use stolen credit card information or fake identities to make purchases online, causing financial losses for both consumers and merchants. For example, in 2017, hackers stole the personal information of over 143 million customers from Equifax, a major credit reporting agency in the US. The breach exposed sensitive data such as social security numbers, birth dates, and credit card numbers, putting millions of people at risk of identity theft and financial fraud.
- Another common security risk in digital payment systems is hacking. Cybercriminals can exploit vulnerabilities in payment systems to gain unauthorized access to sensitive data or steal funds. For instance, in 2013, hackers breached Target's payment system and stole the credit and debit card information of over 40 million customers. The attack cost the company millions of dollars in damages and lost revenue, as well as eroding consumer trust in the brand.

- When it comes to protecting yourself while using digital payment systems, there are a few key things you can do. First and foremost, make sure you use strong passwords that are hard for others to guess. This means avoiding common words or phrases, and using a combination of letters, numbers, and symbols. It's also important to avoid using public Wi-Fi when making payments, as this can leave you vulnerable to hackers and other security threats.
  Another important step is to monitor your accounts regularly, so you can quickly spot any suspicious activity. This means checking your bank statements and credit reports on a regular basis, and reporting any unauthorized transactions immediately. By taking these steps, you can help protect yourself from fraud and other security risks when using digital payment systems.

Unified Payment Interface(UPI) and micro ATM's

UPI stands for Unified Payments Interface. It is an instant real-time payment system developed by National Payments Corporation of India (NPCI). **UPI** allows users to make payments to merchants and individuals using their mobile phones.
The UPI has made paying for transactions easier and simpler, facilitating economic movement within the country.

Micro ATM:
This is a small, portable ATM that is typically operated by a Business Correspondent (BC). BCs are individuals or entities that have been authorized by a bank to provide basic banking services to customers in rural and semi-urban areas.
Micro ATMs allow customers to make UPI payments, as well as other transactions such as cash withdrawals and balance inquiries.

Challenges faced during UPI Payments

- **Security concerns:** UPI transactions are secure, but there have been some reports of fraud. This is a challenge that needs to be addressed in order to build trust in the system.
- **Interoperability:** UPI is a bank-led system, which means that not all banks support it. This can be a challenge for users who want to use UPI with a particular bank.
- **Accessibility**: UPI requires a smartphone and internet connection. This can be a challenge for people in rural areas who may not have access to these resources.

Challenges faced during Micro ATM Payments

- **Intermediary fees**: Micro ATM transactions often incur higher fees than other digital payment methods. This can be a barrier for people who are on a tight budget.
- **Fraud**: Micro ATMs are sometimes used for fraudulent activities. This is a challenge that needs to be addressed in order to protect users.
- **Acceptance:** Micro ATMs are not as widely accepted as other digital payment methods. This can be a challenge for people who want to use them in shops and other businesses.

Despite these challenges, UPI and micro ATM payments are still two of the most promising digital payment methods in India. With continued innovation and investment, these methods can help to make digital payments more accessible, secure, and convenient for everyone.

Here are some suggestions for how to address the challenges faced by UPI and micro ATM ` payments:

Security: UPI and micro ATM providers can implement additional security measures to protect users from fraud. This could include things like two-factor authentication and fraud detection systems.

Interoperability: UPI and micro ATM providers can work together to make their systems more interoperable. This would make it easier for users to use UPI with any bank and micro ATMs with any provider.

Accessibility: UPI and micro ATM providers can work to make their systems more accessible to people in rural areas. This could include things like providing subsidies for smartphones and internet access.

Intermediary fees: UPI and micro ATM providers can work to reduce the fees charged for transactions. This would make these methods more affordable for people on a tight budget.

Acceptance: UPI and micro ATM providers can work to increase the acceptance of their systems by businesses. This could include things like offering incentives to businesses that accept these methods.

By addressing these challenges, UPI and micro ATM payments can become even more popular and effective digital payment methods in India.

Bharat QR & BHIM App

Introduction

In today's digital era, cashless transactions have gained significant momentum. Digital payment systems have revolutionized the way we conduct financial transactions, providing convenience, speed, and security. In this presentation, we will delve into two prominent digital payment methods: Bharat QR Code and Bharat Interface for Money (BHIM) App. We will explore their features, benefits, and security aspects.

Bharat QR & BHIM App

- **Bharat QR** is a revolutionary payment system that allows users to make digital payments using their smartphones. Bharat QR Code is a standardized QR code payment system introduced by the National Payments Corporation of India (NPCI). It enables users to make payments by scanning QR codes displayed at merchant outlets or websites.

- **BHIM App** is a revolutionary digital payment system that has been developed by the National Payments Corporation of India (NPCI). It allows users to make instant payments using their mobile phones, without the need for cash or credit cards. With BHIM App, users can easily transfer money to anyone with a UPI ID or mobile number, pay bills, and even recharge their mobile phones.

How They Work And Their Benefits

How They Work

1. A customer scans the QR code using a compatible payment app on their smartphone.
2. The app decodes the QR code and retrieves payment details such as merchant ID and transaction amount.
3. The customer confirms the payment and authorizes the transaction using their preferred payment method, such as a linked bank account or mobile wallet.
4. The payment is processed, and a confirmation notification is sent to both the customer and the merchant.

Benefits

1. **Convenience**: Eliminates the need for physical cash, cards, or POS terminals, allowing seamless and contactless payments.
2. **Wide Acceptance**: Accepted by a vast network of merchants, including small businesses, without the need for additional infrastructure.
3. **Interoperability**: Supports multiple payment methods, such as debit cards, credit cards, UPI, and digital wallets.
4. **Security**: Provides secure transactions with end-to-end encryption and tokenization of sensitive information.

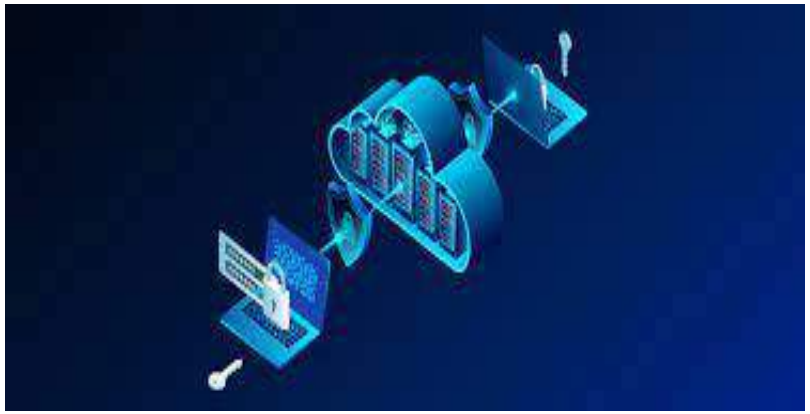
ROLE OF CYBER SECURITY

Paying through Bharat QR and BHIM App involves various technologies to ensure a secure and efficient transaction process. They are:

1)QR Code Encoding &Decoding : To generate a Bharat QR Code, computer algorithms are used to encode and decode payment-related information such as the merchant's identifier, transaction amount, and other details into a QR code format.

2) Network Communication & Encryption : The payment app utilizes network protocols (such as HTTPS) to securely communicate with the merchant's server and cryptographic algorithms (such as SSL/TLS) are employed to encrypt the data.

3)Backend Systems & Data Validation and Verification : This involves using APIs (Application Programming Interfaces) to facilitate secure transaction processing. The payment gateway performs validation and verification ensuring the accuracy of the information.



4)User Authentication & Tokenization : The payment app incorporates user authentication mechanisms such as PINs, biometrics, or passwords to ensure that only authorized users can initiate transactions. Sensitive information, is replaced with unique tokens during the transaction process. This reduces the risk of data breaches.

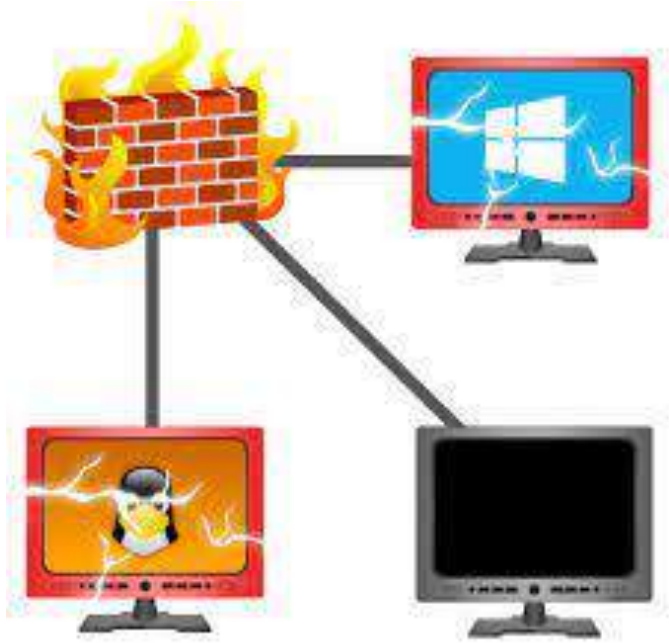
5)Secure Storage: Sensitive user data, such as transaction history or payment details, must be stored securely using encryption and access control mechanisms to prevent unauthorized access.

CYBER THREATS IN BHARAT QR AND BHIM APP

1) **Malicious Apps:** Users may unknowingly download malicious apps that mimic legitimate payment apps, which can steal sensitive information, including login credentials and transaction details.

2) Impersonation: Attackers can pose as legitimate organizations or individuals to deceive users into sharing confidential information, such as OTPs or bank account details, by phone calls, messages, or emails.

3) Man-in-the-Middle (MitM) Attacks: Attackers intercept and alter communication between the user's device and the payment infrastructure, allowing them to capture sensitive information or modify transaction details.



4) **Credential Theft:** Attackers may employ various methods, such as keyloggers or phishing, to steal user login credentials for the Bharat QR or BHIM App, enabling them to gain unauthorized access to user accounts.

5) **Insider Threats:** Unauthorized access or malicious actions by employees or insiders with privileged access to the systems may lead to data breaches or compromise user information.

6) **Outdated Software**: Using outdated versions of the Bharat QR or BHIM App or operating systems on mobile devices can leave users vulnerable to known security vulnerabilities that attackers can exploit.

BEST PRACTICES FOR CYBER SECURITY

1) **Download and Update Securely** : Ensure you download the official Bharat QR or BHIM App from trusted sources like official app stores and keep the app and your mobile device's operating system up to date with the latest versions to benefit from security patches and bug fixes.

2)Avoid suspicious links: Be wary of clicking on links from unknown sources, as they may lead to phishing websites or malware downloads.

3) **Strong Authentication and Passwords**: Create strong, unique passwords for your Bharat QR or BHIM App account, and avoid using easily guessable information. Whenever available, enable multi-factor authentication to provide an additional layer of security to your account.

4)Avoid public Wi-Fi networks: Refrain from using public Wi-Fi networks for transactions, as they are often unsecured and prone to interception. Instead, use secure networks or your mobile data connection.

5) **Regularly review transactions:** Keep a close eye on your account activity and transaction history to detect any suspicious or unauthorized transactions. If you notice any unusual or unauthorized activity, promptly report it to the appropriate authorities or your bank.

CONCLUSION

In conclusion, Bharat QR and BHIM app are powerful tools that have revolutionized the way we make digital payments. However, with great power comes great responsibility, and it is important to be aware of the cybersecurity threats that come with using these apps.

We discussed various cybersecurity threats such as phishing, malware, and hacking, and suggested preventive measures such as using strong passwords, enabling two-factor authentication, and keeping devices updated. We also provided some best practices such as avoiding public Wi-Fi, not sharing personal information, and reporting suspicious activities.

DIGITAL PAYMENTS: Merits and De Merits

WHAT LEAD TO DIGITAL PAYMENTS

How did we come to a point that digital payment is everywhere ?

A BRIEF LINE OF EVENTS

1990s

With the rise of the internet , banks offered online banking services

2000's

Introduction of Credit Cards and Debit Cards

2010

Introduction of UPI

2016

Demonetization lessened the presence of hard cash

2020

A surge in digital payments due to the pandemic

DEMONETISATION

- Demonetisation left a blatant impact on the digital payments in the country. Some of these Impacts are:

- **Surge in digital transactions:** Demonetization led to a sudden shortage of cash in circulation, prompting people to adopt digital payment methods to meet their daily transaction needs.

- **Rise of Unified Payments Interface (UPI):** The popularity of UPI soared after demonetization, providing a seamless and instant way for users to transfer money and make payments using their smartphones.

- **Shift in consumer behavior:** Demonetization prompted a behavioral shift among consumers, who became more accustomed to digital payments and started preferring them over traditional cash transactions.

COVID -19 AND ITS IMPACT

- ***Accelerated digital transformation:*** The pandemic had accelerated the adoption of digital payment methods. It made sure businesses embraced cashless transactions that increased efficiency and convenience

- ***Contactless Payments :*** Due to the virus spreading with touch, many offline shops had to shift contactless payments. For example , there was a new set of cards introduced with a WIFI option that could pay bills up to 5000 rupees with the tap of the card.

- ***Boost to Online Businesses :*** The pandemic ensured no one stepped out of their houses. But this didn't stop business as they shifted towards e-commerce sites and online businesses. This made sure that the products were still bought by the customer.

SOME MODES OF DIGITAL PAYMENT

How are digital payments used in our day to day lives?

MODES OF DIGITAL PAYMENTS

UPI	Bank Cards	Mobile Wallets	Mobile Banking	USSD
It stands for United Payment Interface. It brings about various bank accounts into a single platform. A customer needn't have multiple apps	Credit and Debit cards with the help of the card number can be used to pay or transfer money digitally .	It enables users to carry cash digitally. Some of the popular mobile wallets are PayTm, PhonePe etc	There are official sites and official apps of the bank which have actions that can help you configure your account.	Stands for Unstructured Supplementary Standard Data. One can dial *99# to avail bank services like fund transfer

UNIFIED PAYMENT INTERFACE

- The UPI is a payment system developed by the NPCI(National Payments Corporation of India) , which facilitates real time money transfer between different banks through mobiles .
- UPI's QR codes enables easy and secure payment by scanning QR codes at the merchant outlets. This form of payment is found everywhere and has become widely popular.
- UPI is a single interface to link multiple bank accounts to a single UPI id. This feature makes sure you don't need to remember account details for all banks

MERITS AND DEMERITS OF DIGITAL PAYMENTS

What changed after the introduction of digital payments ??

MERITS

- ***Convenience:*** Digital payments provide a quick and hassle-free way to make transactions anytime and anywhere, eliminating the need to carry physical cash.

- ***Speed:*** Electronic transactions are processed instantly, allowing for real-time fund transfers and faster payment settlements compared to traditional banking methods.

- ***Transparency:*** Digital payment systems maintain detailed transaction records, enhancing transparency and simplifying financial tracking and management.

- ***E-commerce Growth:*** Digital payments have fueled the growth of e-commerce by providing a secure and efficient way for consumers to make online purchases.

MERITS

- Some of the important advantages other than the ones mentioned above are mentioned in the image beside.

- ***Cost-effectiveness***: Digital transactions often incur lower fees and maintenance costs than traditional banking methods.

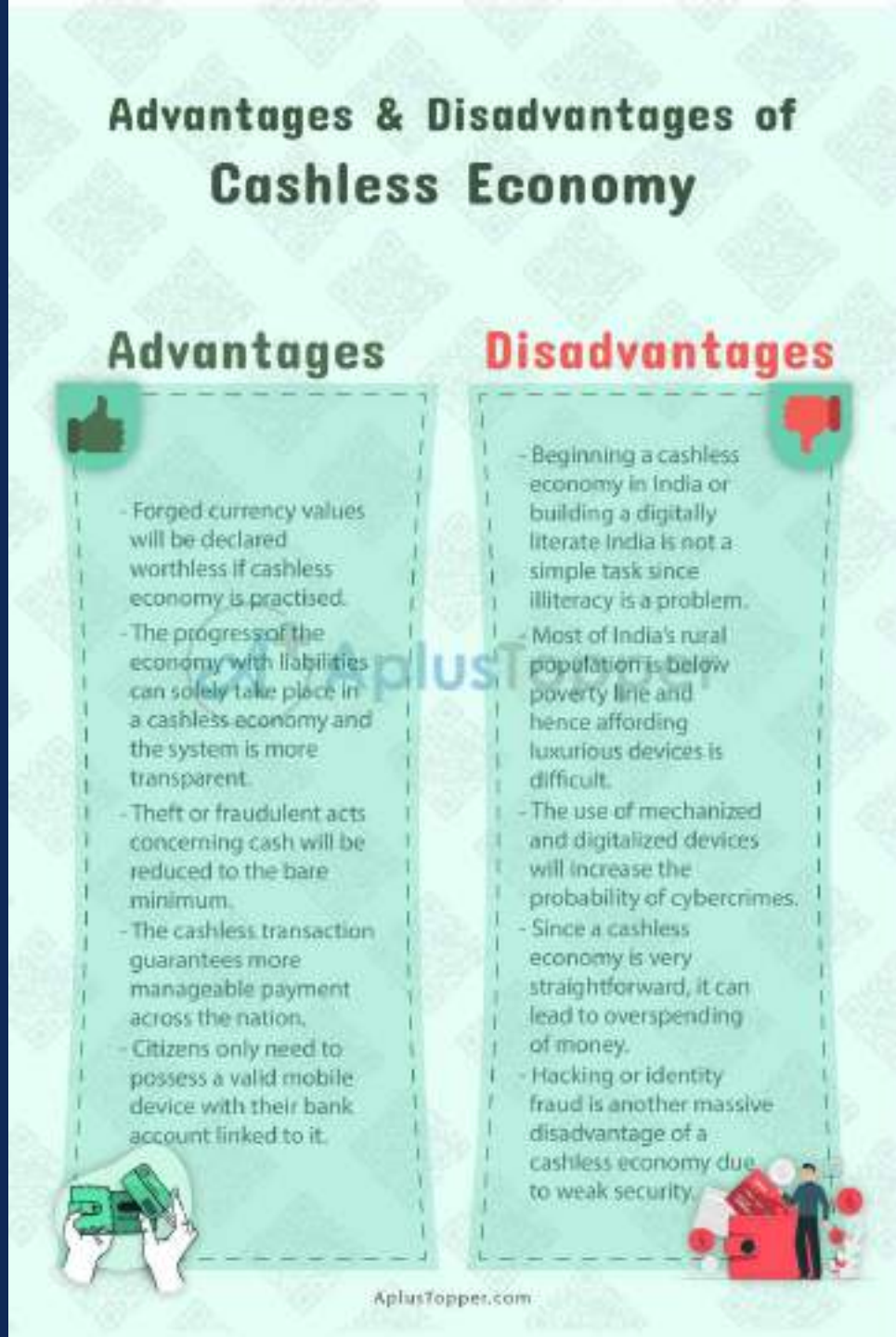
- ***Loyalty Programs and Rewards:*** Digital payments especially mobile banking and internet banking platforms offer reward points that are given on the basis of how much money you've spent using that platform.

DEMERITS

- ***Exclusion of Unbanked Population:*** Despite efforts towards financial inclusion, a significant portion of the population remains unbanked or lacks access to smartphones, excluding them from digital payment services.

- ***Cybersecurity Risks:*** Digital payments are vulnerable to cyber threats, including hacking, phishing, and data breaches, potentially exposing sensitive personal and financial information.

- ***Privacy Concerns:*** Digital payment platforms collect user data for transaction processing and analysis, raising concerns about privacy and data protection.



DEMERITS

- ***Transaction Failures:*** Technical glitches or system downtime can lead to transaction failures, causing inconvenience and frustration for users.

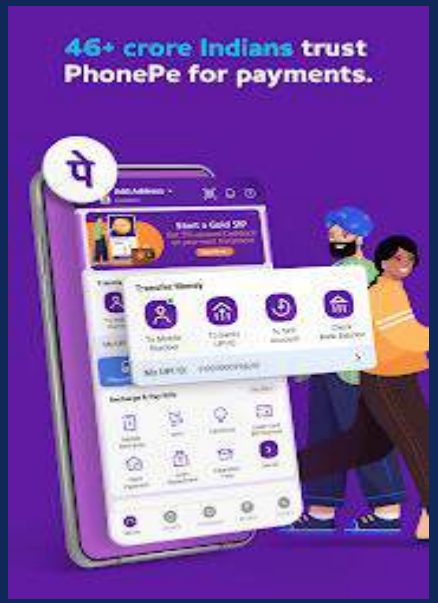
- ***Fraud and Scams***: Fraudulent activities, such as unauthorized transactions and identity theft, can occur in digital payment systems, impacting consumer trust.

- ***Regulatory Concerns:*** Rapid advancements in digital payments may outpace regulatory frameworks, leading to potential gaps in oversight and consumer protection.

CASE STUDY: PHONE PE

- PhonePe is an Indian digital payments and financial services company headquartered in Bengaluru, Karnataka, India. PhonePe was founded in December 2015, by Sameer Nigam, Rahul Chari and Burzin Engineer. The PhonePe app, based on the Unified Payments Interface (UPI), went live in August 2016.
- The PhonePe app is available in 11 Indian languages. Using PhonePe, users can send and receive money, recharge mobile, DTH, data cards, make utility payments, pay at shops, invest in tax saving funds, liquid funds, buy insurance, mutual funds, and digital gold.
- In 2022, PhonePe became the first UPI TPAP (Third Party Application Providers) App to allow UPI activation through Aadhaar.

PhonePe
INDIA'S PAYMENTS APP



WHAT NEXT ?

- ***Cryptocurrency and Blockchain:*** Cryptocurrency is a digital currency, which is an alternative form of payment created using encryption algorithms. The use of encryption technologies means that cryptocurrencies function both as a currency and as a virtual accounting system.

- ***QR code Innovations:*** Advancements in the QR industry, can help make transactions more safer and faster.

- ***Contactless and Wearable Payments:*** Continued growth of contactless payments via smartphones, wearables, and connected devices for a seamless experience.

- ***Biometric Authentication:*** Enhanced security through biometric verification like fingerprints and facial recognition for seamless yet secure transactions.


Thank you