BCA

Semester: V

MIS AND E-BUSINESS

E-Payment Systems

REFERENCE NOTE

Unit-5: E-Payment Systems

- Online payment cards (credit cards, charge cards, debit cards, smart cards), processing cards in online
- Credit card payments procedure,
- e-micropayments,
- e-checks and its processing in online.
- Automated clearing house (ACH) network,
- mobile payments (Digital wallet),
- mobile payment participants and issues,
- International payments, emerging EC payment systems and issues: crypto currency, virtual currency.

Electronic Payment System

- E-payment or Electronic payment is any digital financial payment transaction involving currency transfer between two or more parties
- Financial exchange that takes place online between buyers and sellers.
- It used for serve customer faster and lower cost.
- Every business look for prompt, secure payment and clearing and settlement of credit or debit claims as fast as possible.

- Electronic payment system is a system which helps the customer or user to make online payment for their shopping.
- Delay payment cause to be disrupted entire business chain.
- Electronic payments are far cheaper than the traditional method of mailing out paper invoices and then processing payments received.
- Implementation of electronic payment systems is in its infancy and still evolving

Advantages:

- Decreasing technology cost:
- Reduced operational and processing cost:
- Increasing online commerce:

Some examples

- Online reservation (irctc) (Indian Railway Catering and Tourism Corporation)
- Online bill payment (ntc,ncell)
- Online order placing (flipkart)
- Online ticket booking (movies)

Online payment system:

Payment cards are electronic cards that contain payment-related data.

1. **Credit cards.** A credit card enables its holder to charge items (and pay later) or obtain cash up to the cardholder's authorized limit. With each purchase, the credit card holder receives a loan from the credit card issuers. Most credit cards do not have an annual fee. However, holders are charged interest if the balance is not paid in full by the due date. Visa and MasterCard are the leading cards.

2. Charge cards. These are special credit cards where the balance must be paid in full by the due date and usually have annual fees. Examples of issuers are American Express and Diner's Club (they both offer regular credit cards as well).

3. Debit cards. Payments made with a debit card are withdrawn from the holder's checking or savings account. The actual transfer of funds usually takes place in real time from the holder's account (if an ATM card is used). However, a settlement to a merchant's checking account may take place within one to 2 days. Again, MasterCard and Visa are examples of debit card issuers. For a discussion of some best practices for debit card usage.

4. SMART CARDS

A smart card is a plastic payment card that contains data in an embedded microchip. The embedded chip can be a microprocessor combined with a memory chip or just a memory chip with nonprogrammable logic. Information on a microprocessor card can be added, deleted, or otherwise manipulated; a memory-chip card is usually a "read- only" card, similar to a magnetic stripe card. The card's programs and data must be downloaded from, and activated by, some other device (such as an ATM). Smart cards are used for a wide variety of purposes including:

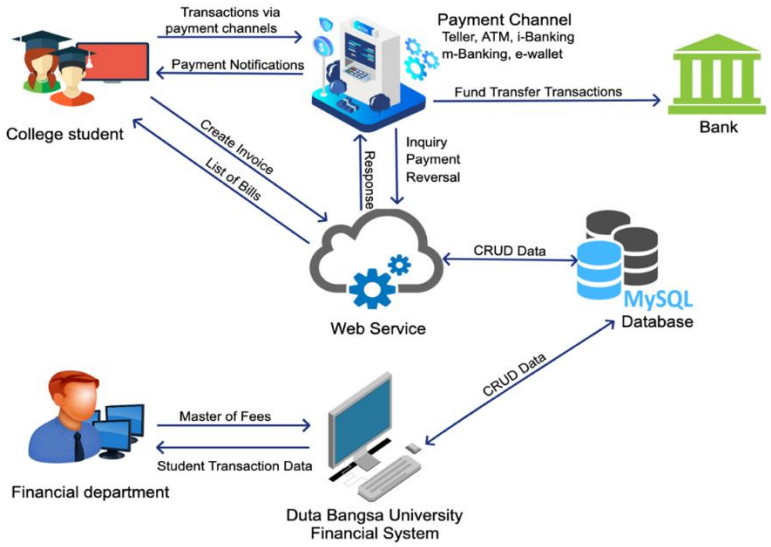
- Telecom-SIM cards
- Financial-cards issued by banks, retailers, and service providers for payment services (debit, credit, prepaid), loyalty, and social cards with payment apps
- Government and healthcare-cards issued by governments for citizen identification and online services and cards issued by private health insurance companies

- Device manufactures-mobile phones, tablets, navigation devices, and other connected devices including secure element without SIM application
- Others cards issued by operators for transport, tolls, car park service, pay Tand physical and logical access to cards.

Processing Cards Online

The processing of credit card payments has two major phases: authorization and settlement. Authorization determines whether a buyer's card is valid (e.g., not expired) and whether the customer has sufficient credit or funds in his or her account. Settlement involves the transfer of money from the buyer's account to the merchant's. There are a number of parties involved in both processes including.

- **Customer.** The individual possessing the card.
- **Merchant.** The vendor that sells goods or services.
- **Issuing bank.** The issuer (usually a bank) of the credit (debit) card to customer (or businesses). Services customer accounts including billing and collecting month payments.
- **Merchant acquiring bank.** Enrolls merchants into a program that accept a specific card brand (e.g., Visa) and, on the merchant's behalf, processes debit or credit card payments made using that particular card brand.
- **Credit card (association) network**. Credit card networks determine where credit cards can be used and facilitate the payment process between credit card users, merchants, and credit card issuers.
- **Payment service provider.** The company that provides electronic connections and transaction services among all the parties involved in electronic payments (including authorizations). A payment service provider is also called a payment gateway provider.



Authorization cycle-The Customer initiates a payment transaction (fills out Web page, swipes a card, etc.). The merchant receives the transaction information. This information is passed to its PSP where it is routed to the merchant's acquiring bank (processor). The acquiring bank passes the information to the issuing bank through the credit card network. If the issuing bank approves the transaction, an authorization code is sent back to the merchant via the same linkages. The issuing bank also holds an authorization associated with that merchant and consumer for the approved amount. Finally, the merchant notifies the customer and fulfills the order.

Settlement-At the end of the day, the merchant submits in batch all the approved authorizations they have received to the acquiring bank via its PSP. Again, the acquiring bank makes the batch settlement request to the

issuing bank via the card network. The credit card issuer makes a settlement payment to the acquiring bank via the card network.

- EC micropayments
- Micropayments or e-micropayments are small payments made online, usually under $10. From the viewpoint of many vendors, credit cards are too expensive for processing small payments. The same is true for debit cards, where the fixed transaction fees are greater, even though there are no percentage charges.

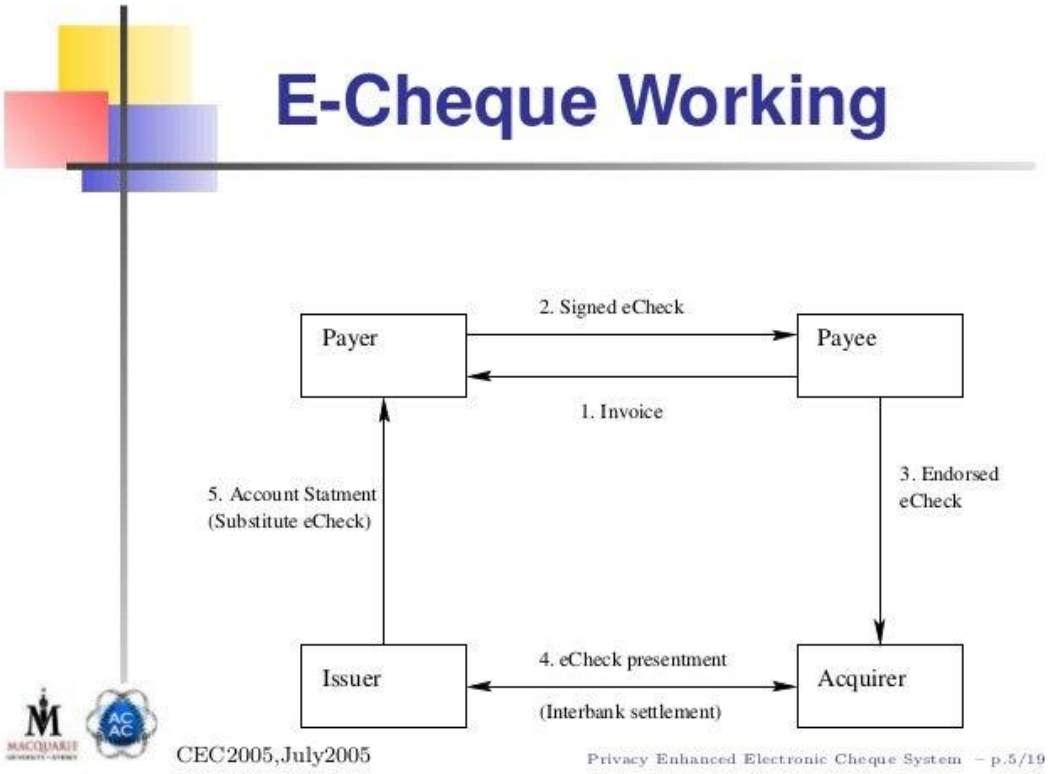
Micropayment Models

- There are five basic micropayment models that do not depend solely or directly on credit or debit cards and that have enjoyed some amount of success. Some of these are better suited for offline payments than online payments, although there is nothing that prevents the application of any of the models to the online world. The models include:

- **Aggregation.** Payments from a single consumer are accumulated and processed periodically (e.g., once a month), or as a certain level is reached (e.g., $100). This model fits vendors with a high volume of repeat business. Both Apple's iTunes and App Store use this model. The transportation card used in Seoul, Korea, and many other places is of this nature.
- **Direct payment.** In this case, an aggregation is used, but the micropayments are processed with an existing monthly bill (e.g., a mobile phone bill).
- **Stored-value.** Funds are loaded into a debit account from which the money value of purchases is deducted when purchases are made. This system is being used by several online gaming companies and social media sites.
- **Subscriptions.** A single payment (e.g., monthly) provides access to content. Online gaming companies and a number of online newspapers and journals have used this model.
- **A la carte.** Payments are made for transactions as they occur; volume discounts may be negotiated. This model is used in stock trading, such as at E-Trade.

E-checks and its processing in online

- An electronic version or representation of a paper cheque. The account holder writes an e-check (or e-cheque) using a computer or other type of electronic device and transmits the e-cheque to the payee electronically.
- Like paper cheques, e-checks are signed by the payer and endorsed by the payee. Rather than handwritten or machine-signatures, however, e-checks are affixed with digital signatures, using a combination of smart cards and digital certificates.
- The payee deposits the e-check, receives credit, and the payee's bank clears the e-check to the paying bank. The paying bank validates the e-check and then charges the cheque writer's account for the cheque.
- Additionally, it has more security features than standard paper checks including authentication, public key cryptography, digital signatures, and encryption, among others.



Automated clearing house (ACH)

- In the United States, the ACH Network is the national automated clearing house for electronic funds transfers. It processes financial transactions for consumers, businesses, and federal, state, and local governments. ACH processes large volumes of credit and debit transactions in batches.
- **Nepal Clearing House Limited (NCHL),** a subsidiary of the Central Bank of Nepal, has implemented an Electronic Check Clearing (ECC) system in the Nepal. The introduction of ECC has drastically reduced the time required to clear the checks from a few days to minutes. Currently, 140 banks and financial institutions' 1200 branches across the country use our system. Checks are cleared at the branch level itself. Integrated Solutions partnered with ProgressSoft Corporation, Jordan, for the supply and implementation of ECC solution in Nepal.
- **Electronic Cheque Clearing (NCHL-ECC)** is an image-based, cost-effective, MICR cheque processing and settlement solution where an original paper cheque is converted into an image for electronic processing of the financial transactions between participating member Banks/FIs. The physical movement of the cheques are truncated or stopped at the level of the presenting bank in the NCHL-ECC System. The cheque does not physically travel to the clearing house or to the paying branch as it used to do in manual clearing process resulting in a faster and easier processing of the cheque transactions.

Mobile payments (Digital wallet)

- The term mobile payment refers to payment transactions initiated or confirmed using a person's mobile device, usually a smartphone although payments can be made with other mobile devices such as tablets and wearables. The term actually covers a number of different types of solutions, as well as different combinations of hardware and software technologists.
- Mobile payments are a popular method for government's payments to people, especially in developing countries, such as India and Brazil, where more people have smartphones than bank accounts.

- "Digital Wallet" also known as a "mobile wallet" or an "e-wallet" which is an online service or system that can stores user's payment information. It can be used to making micro-electronic transaction. we can make such transactions via the internet, SMS, or a mobile app, after simple steps for registration. Example for international online payment platforms like Google Pay, Samsung Pay, Facebook Pay, etc. in context of Nepal eSewa, Khalli, IME Pay, PrabhuPay, QPay Nepal etc.
- The term mobile digital wallet refers to the combination of an electronic account along with a smartphone and mobile app designed to make purchases digitally and to redeem rewards from loyalty programs and targeted digital promotions. There are two main types of wallets-device-based and cloud-based.

Device-Based Digital Wallets

- These are proximity payment systems enabled by near-field communication (NFC) technology.
- On the consumer side, the system requires that the mobile device being used is equipped with NFC antenna and an integrated chip or a smart card inside the phone that holds payment card information (credit or debit).
- On the merchant's side, it requires a specialized NFC reader used to recognize the chip when the chip comes within a short distance of the reader and a network for handling the payment.
- Essentially, a buyer first enters his or her credit card information into the wallet app on the phone prior to shopping. At the time of the purchase, the buyer then "waves" the specially equipped mobile phone near a reader to initiate a payment. The reader collects the info and passes to the payment network. The card is charged and the purchase is complete.
- These proximity payments are also called contactless payments where the phone plays the surrogate roll of a contactless card with a chip.
- The most popular are PayPal wallet (paypal.com), Apple Pay (apple.com/apple- pay) and Android Pay (android.com/pay)."

Cloud-Based Digital Wallets

- An alternative to device-based mobile wallets is cloud-based mobile wallets. The infrastructure for these wallets is not as onerous as a system based on NFC.
- Basically, a customer enrolls his or her card with a secure Web service. Requests for payments are made to the service and charged to enrolled card(s).
- In this way no card information is transmitted during a purchase. Instead, transactions are initiated by scanning a barcode or Quick Response (QR) code created specifically for the customer and stored and displayed on the smartphone by wallet app. A QR code is a 2D barcode consisting of a collection of black square dots placed on a square grid with a white background.
- What is required on the merchant's end is a barcode or QR code image reader that is networked into the service via the Web. The whole system operates much like the way PayPal operates without using a Web page with a PayPal button to start the process. Instead, it's started when the code is scanned. As a point of fact PayPal employs a cloud-based mobile wallet instead of device-based.

Mobile payment participants and issues:

Just like online payments, there are many parties involved in any mobile payment system. From the stand point of the various parties, any successful mobile system needs to overcome the following sorts of issues:

- **Consumer.** Buyer pays a merchant for goods and services. This is the purview of most digital wallets (e.g., Apple Pay, e-sewa).
- **Merchant.** Receiving money from a customer in exchange for goods and services. Often enabled by mobile POS (e.g.,Square).

- **Person-to-person (P2P).** Money exchange between two or more people, as a gift or payback (e.g., PayPal's Venmo).
- **Institutional**. Managing and paying bills from an institution (like a utility company) for services rendered (e.g., Finovera or Mint).

Mobile payment issues:

For buyer: Security (fraud protection), privacy, ease of use, and choice of mobile device.
For Seller. Security (getting paid on time), low cost of operations, adoption by sufficient number of users, and improved speed of transactions.
For network operator: Availability of open standards, cost of operation, interoperability, and flexibility and roaming.
For financial institutions: Fraud protection and reduction, security (authentication, integrity, nonrepudiation), and reputation.

International payment system

International payments consists of outgoing and incoming payments in a country's currency out of and into that country, as well as offshore payments in that currency, between two parties outside that country. A global payment and settlement system exists for each national currency. For payments between distant parties over such a system to function like the face-to-face delivery of cash, a robust banking system, tight risk controls, and sophisticated technological and liquidity-saving features must be put in place.

- **Visa**
- Visa Inc. is an American multinational financial services corporation headquartered in Foster City, California, United States. It facilitates electronic funds transfers throughout the world, most commonly through Visa-branded credit cards, debit cards and prepaid cards.
- Visa cards are available to individual and business customers through a range of financial institution partnerships. Financial institutions can choose between a numbers of network service providers for transaction processing and card branding.
- Visa is a prominent processing network and their cards are accepted by businesses in more than 200 countries and territories across the world.
- Visa partners with companies across the world to facilitate transaction processing for both banks and merchants. Financial institutions and fintech companies can establish service agreements with Visa for branded cards that use the Visa network. Service agreements include bank transaction fees and Visa network charges. Visa also partners with merchants through varying types of service agreements.

MasterCard

- The MasterCard business is responsible for one of the four largest payment networks in the global payments industry.
- MasterCard partners with institutions all over the world to offer MasterCard branded network payment cards.
- MasterCard payment cards exclusively use the MasterCard network for processing all transaction communications. Payment cards may be credit, debit, or prepaid cards.
- MasterCard is a payment network processor.

- MasterCard partners with institutions to issue MasterCard payment cards that are processed exclusively on the MasterCard network.
- MasterCard's primary source of revenue comes from the fees it charges issuer based on each card's gross dollar volume.

American Express Card

- An American Express card, also know à as an "AmEx," is an electronic payment card branded by the publicly-traded financial services company American Express (AXP).
- American Express issue and processes prepaid, charge, and credit cards. American Express cards are available to individuals, small businesses, and corporate consumers in the U.S. and around the world.
- American Express cards are issued by American Express-a publicly-traded financial services company-and are credit cards or charge cards.
- An American Express card, also called an AmEx, can offer a variety of perks, including rewards points, cashback, and travel perks. Some cards are co-branded, such as those with Delta and Hilton.
- American Express is one of the few companies that issue cards and has network to process card payments. Both Visa and MasterCard have processing networks but they don't issue cards.

Discover Card

- Discover Card is a credit card brand known for its pioneering cashback rewards program, and is one of the most accepted credit card brands in the and around the world.
- Discover Card is a brand of credit card offered by Discover Financial Services. Discover is one of the largest credit card brands in the U.S. and around the world, alongside Visa, MasterCard, and American Express.
- In contrast to Visa and MasterCard, Discover issues its credit cards directly through its own Discover Bank. As of 2016, Discover was the sixth-largest credit card issuer in the U.S., and the most widely-accepted credit card brand around the world.

PayPal

- PayPal is an electronic commerce (e-commerce) company that facilitates payments between parties through online funds transfers. PayPal allows customers to establish an account on its platform, which is connected to a user's credit card or checking account. Once identification and proof of funds have been confirmed, a user may begin sending or receiving payments to and from other PayPal accounts.
- PayPal attempts to make online purchases safer by providing a form of payment that does not require the payer or payee to disclose credit card or bank account numbers.
- PayPal is an online payments platform that offers individuals and businesses low- cost transnational services.
- Once owned by eBay, PayPal has been its own company since 2015.
- In addition to online payments, PayPal also offers a variety of related services including debit cards for payments, credit card readers for small merchants, and lines of credit.
- PayPal is considered a very secure method of sending payments online.

As a PayPal member, you are able to:

- Transfer money from your bank account to your PayPal account
- Get a cash advance from your credit card and deposit the amount in your PayPal account.
- Transfer money from your own PayPal account to another member's PayPal account
- Transfer money from your PayPal account to your checking or savings account
- Have a check mailed to you for the balance of your PayPal account
- Get a PayPal debit card that you can use to make real-world purchases from your PayPal account.

Benefits of Using PayPal

- PayPal is a fast and easy way to buy things online. PayPal is the preferred method of payment on many shopping websites, besides just eBay. PayPal offers these seven benefits:
- **Flexibility for Sellers.** With a PayPal membership, even very small volume sellers can quickly and easily accept payments that originate from buyers' credit or debit cards.
- **Speed.** PayPal transfers between sellers are instant, and transfers from PayPal accounts to bank accounts can take as little as 24 hours.
- **Affordability.** The fee to use PayPal is 30 cents per transaction, plus 3% of the total amount of the transaction.
- **Safe Buying.** Because PayPal offers buyer guarantees and a specific process for disputing transactions, so users always have recourse whether they are a buyer who didn't get what they ordered or a seller who may worry she will be stiffed on payment.
- **Account Privacy** PayPal is secure. For buyers, this means a level of account protection not offered by brick-and-mortar stores, where retailers commonly have buyers' account information in-hand after purchases.
- **Ease of Record Keeping.** PayPal history goes back to the day the account was opened. Users also have the ability to pull reports and users are provided with a 1099 if they have more than 200 transactions and $20,000 in sales.
- **Acceptance Online.** PayPal is now a common method of payment on many shopping websites as well as websites that take payment for any other reason.

Emerging EC payment systems and Issues: currency, virtual currency.

Physical vs Digital

- To the differences among these three concepts, let us start at the other end of the currency spectrum-fiat currency. Fiat currency (aka real currency, real money, or national currency) is the "coin and paper money of a country that is designated as legal tender, circulates, and is customarily used and accepted as the medium of exchange in the issuing country and other countries.
- Electronic money (abbreviated e-money) is a digital representation of fiat currency used for purposes of electronic transfer (e.g., the digital representation funds used to settle a merchant account after an EC purchase is made).
- In contract virtual currency is the "digital representation of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal status in any jurisdiction."
- Basically, it only functions as a currency because there is a community of users willing to treat it as such.

- Finally, digital currency is a generic term that refers to the digital representation (0 s and l s) of either e-money (fiat) or virtual currency (non-fiat). So, e-money and virtual currency are types of digital currency but not vice versa.

Virtual Currency

- Virtual currency covers two sub-types: nonconvertible (closed) and convertible (open). According to the US Treasury's Financial Crimes Enforcement Network (fincen.gov, convertible virtual currency is a virtual currency that has "an equivalent value in real currency, or acts as a substitute for real currency." Some examples include the cryptocurrencies like Bitcoin and most retail e-coupons.
- In contrast, a nonconvertible virtual currency is a virtual currency used in a specific virtual world or domain that cannot (theoretically) be exchanged for fiat currency. Many of the better known examples come from online games. Some examples of this would include World of Warcraft Gold, Farm(ville) Cash, and Q Coin from Tencent QQ.
- In these games, success is based on obtaining virtual money, which is earned by completing various tasks or purchased using real money (which is often the primary source of income for the game company).
- Technically, these currencies cannot be used or exchanged in the outside world. However, in many cases secondary markets (black or not) have arisen that are willing to exchange the nonconvertible currency into a fiat currency or some other virtual currencies.
- A key feature of nonconvertible, virtualized currencies is that they are centralized. This means that there is a single administrative authority in charge of regulating the currency-issuing the currency, establishing rules of use and exchange rates, tracking payments, and controlling the amount in circulation.
- In contrast convertible virtual currencies can be either centralized or decentralized. A decentralized virtual currency is distributed, open- sourced, and peer-to-peer. There is no single administrate authority who oversees and monitors the currency. This is the nature of many of the cryptocurrencies like
- Bitcoin

Bitcoin and Other Cryptocurrencies

- Bitcoin is an encrypted, decentralized (peer-to-peer), convertible, virtual currency.
- The origin of Bitcoin comes from a specification and proof of concept developed in 2009 by Satoshi Nakamoto and published in a paper entitled "Bitcoin: A Peer-to- Peer Electronic Cash System." That is not his real name, it's a pen name.
- The real identity of the inventor is still unknown. After the initial development, Satoshi left the project in the hands of a community of open source developers (see bitcoin.org), meaning that the development and maintenance of the underlying code is being done by a community in much same ways as projects like Linux and Apache.
- Bitcoin was not the first system to propose a decentralized virtual currency. However, it was the first to come up with a decentralized system that offered a usable solution to what is known as the double-spend problem. As the concept implies, in a virtual currency double-spending refers to the result of spending the same money more than once.
- In most systems, double spending is handled by having a central (automated) authority review transactions before they are committed. In Bitcoin, there is no central authority, but it relies on an

innovative proof-of- work scheme that uses consensus among peer-to-peer nodes to verify transactions and to protect against assaults like double-spending.

- When we speak about the unit of currency in this system, it is designated in small letters ("bitcoin") which in abbreviated form is designated as BTC (similar to USD).
- There is an upper limit on the number of bitcoins that can be produced (21 million BTC), a governor on the number of bitcoins that are produced on the average every 10 min (i.e., 1 block), and an end date for their production (2040).

Bitcoin Characteristics

- **Durable-**This means that it retains its shape, form, and substance over an extended period of time, so that in the future it will still work as a medium of exchange. While bitcoins have only been around for 7 years, they are widely accepted at merchants, traded on currency exchanges, recognized (or tolerated) by many countries, and owned by sizeable numbers of individuals. There's no assurance about its future, but it has lasted longer than virtually all of its digital predecessors.
- **Divisible-**This characteristic means that a currency can be divided into smaller increments so that the sum of the increments equals the original value. In this way bitcoins can be used to purchase products and services of varying values. The smallest unit of the bitcoin is 0.00000001BTC (that's 1 hundred millionth). This unit is called a Satoshi. It serves the same role as $.01 or a penny in USD.
- **Countable-**This implies that the units are subject to the rules of mathematics so they can be added, subtracted, multiplied, and divided. In accounting terms it means we can employ these operations to measure profit, loss, income, expenses, debt, and wealth and determine the net worth of an entity possessing units.
- **Transportable**-Currency is needed to easily support transactions and exchanges across the world. Because bitcoins run on the Internet is a decentralized fashion, they are more transportable than most fiat currencies.
- **Fungible-**This means that one unit of a currency is interchangeable with all others regardless of when or where it was obtained. For example, in the com commodities market, all No. 2 corn has the same value regardless of where it was grown. Similarly, one bit coin is the same as any other bitcoin regardless of how it was produced or who holds it.
- **Verifiable (non-counterfeitable**)-This means that it is not easily counterfeited, and if it is, it's easily detected. This is one of the key characteristics and strengths of a cryptocurrency like bitcoins. Before any bitcoins are accepted for payment, there is a strong vetting process to ensure its authenticity.

Advantages

- **Anonymity.** Even though transactions are public, there is nothing to tie a user's name to the particular encrypted address or signatures unless the user wants to make the connection public. It's also the case that users can have multiple addresses, even a new one for every transaction. This increases the anonymity. However, the shear fact that transactions and addresses are public leaves open the possibility of tying transactions to real-life identity. For this reason Bitcoin is often referred to as pseudo-anonymous.

- **Simplifying financial transactions**. There are no pre-requisites and no minimum levels required to participate. Transactions between parties can transpire without the assistance of any bank or financial institution. Because transactions are basically frictionless, fees are held to a minimum.
- **Merchant friendly.** For merchants, it's easy to set up a payment system without relying on third-party gateways or intermediaries. The setup costs are minimal and there are none of the chargebacks associated with cards.
- **Supporting cross-border commerce.** Architecturally, Bitcoin can easily support cross-border transactions simply because it utilizes the Internet. Also, it's an open system that allows anyone to join regardless of their location. In most countries they can operate pretty much with impunity largely because of the regulatory confusion over virtual currencies. However, it is the case that Bitcoin is outlawed in a handful of countries (e.g., Russia) and is increasingly subject to the regulations governing banks and institutions in a number of countries, especially those dealing with money laundering and financing terrorism.
- **Free from government manipulation.** In many developing countries and a number of developed countries, the currencies have been subject to governmental fraud and illegal manipulation. On an individual level, accounts have been frozen or expropriated by national governments. On a national level, governments have illegally manipulated the circulation of currency defaulted on debts, etc., all of which impact currency valuations/In Bitcoin no one, governments or otherwise, directs control of accounts, the bitcoins in circulation,, nor their valuation.

Disadvantages

- Not yet widely accepted. Even though there has been substantial growth in the number of merchants accepting Bitcoins, the number of transactions, and the valuations of the currency, it has yet to reach the "critical minimum." The pace may get increasingly slower as governments move to place regulatory controls on aspects like the anonymity of accounts which provides cover for money laundering and the finance of terrorism.
- **Fluctuating valuation**. While all currencies have swings in valuation, the value of a bitcoin has had a history of volatile swings. This means there is substantial risk for owners, much like the risk associated with stock investments. For example, the value went from $120 in October 2013 to $600 in January 2014 to $225 in July 2015, to $408 in November 2015, to $367 in January 2016, to $462 in April 2016. While it's been on the rise lately, there's no assurance that it will continue this way in the future. Besides the risk, this also makes it hard for merchants to know how many bitcoins to charge and how to handle returns. For merchants it is more like dealing with the exchange rates for a foreign currency rather than the domestic currency.
- **Transactions are irreversible.** This is both good and bad. It's bad in the sense that if a buyer makes a purchase and the merchant fails to deliver the goods, there is no recourse because the transactions will already be committed. A variety of external controls have been suggested, but many of them are an anathema to the underlying tenets on which the system operates.
- **Private keys can be lost.** As noted earlier, if a user loses his or her encryption private key(s), they are simply out of luck. Keys can be lost in a variety of inadvertent ways (e.g.. disk crashes, file corruption, stolen hardware, and the like). Even though the transactions and public account numbers are visible, there is no way to sign a message to execute a transaction, and there is no central authority or

administrator who can issue a new key. It's not like losing a password. This is why users are encouraged to back up their private keys to paper or some other medium.

- **Problems with everyday use.** Traditional currencies and cards are easier to use both offline and online and are accepted virtually everywhere. Virtually every online retailer who accepts bitcoins sets their prices in a conventional currencies and determines the bitcoin cost based on exchange rates against those same currencies. So, from the perspective of everyday use, bitcoins offer little advantage.
- **Network latency and issues of scalability.** While the system is designed to verify transactions on average every 10 min, sometimes it can take hours. It is hard to image how this could support the transaction volume of even a reasonable sized retailer or replace a system like Visa that handles thousands of transactions per second.
- Despite these disadvantages, Bitcoin is becoming more popular. There is even a Visa bitcoin card, and its value in dollars is increasing.

Bitcoin Competitors and the Future of Math-Based Currencies

- There are over 700 cryptocurrencies being traded in online markets. Only ten of them have market caps above $10 million, and only three have market caps above $100 million (recall that Bitcoin's was about $7 billion). The three include (coinmarketcap.com):
- **Ethereum (ethereum.org).** Valued at close to $750 million, Ethereum was crowdfunded in 2014 and developed by the Ethereum Foundation, a Swiss nonprofit foundation. While Ethereum is a decentralized blockchain technology that is traded as a virtual currency, it is actually a development platform with its own language that can be used to create other distributed applications like smart contracts that can be run "without any downtime, fraud, or third-party control." In contrast to Bitcoins, it confirms blocks in seconds, not minutes. Recently, Ethereum has partnered with Microsoft to offer Ethereum Blockchain as a service on Microsoft's Azure cloud.
- **Ripple (ripple.com).** Ripple has 35 billion shares versus Bitcoin's max of 21.5 million. Each share is valued at $.007 per share for a market cap close to $230 million. Ripple was originally targeted as a distributed, open source, consensus ledger with its own currency XRP (ripples). More recently, the system has been repurposed for banks and payment networks as a real-time cross-currency settlement system that can support applications like international money transfer.
- **Litecoin (litecoin.com).** Valued at $170 million, this distributed, peer-to-peer cryptocurrency is almost a clone of Bitcoin. Where it differs is it's speed (about 4x faster), its proof-of-work algorithm (called "scrypt" vs. SHA-256"), and the maximum units of currency (84 million vs. 21.5 million).
- While individual cryptocurrencies (including Bitcoin) may fade away, the underlying platforms and algorithms will likely morph to other uses similar to the types of shifts that have occurred with Ethereum and ripple.

The End