1. INTRODUCTION TO CRYPTOCURRENCY

Definition

What is cryptocurrency?

A **cryptocurrency** (or **crypto currency**) is a digital asset designed to work as a medium of exchange that uses cryptography to secure its transactions, to control thecreation of additional units, and to verify the transfer of assets.

Cryptocurrencies are a type of digital currencies, alternative currencies and virtual currencies. Cryptocurrencies use decentralized control as opposed to centralized electronicmoney and central banking systems.

Features of cryptocurrency:

According to Jan Lansky, a cryptocurrency is a system that meets all of the following six conditions:

- Independent: The system does not require a central authority, distributed achieveconsensuson its state.
- Supervision: The system keeps an overview of cryptocurrency units and their ownership.
- Efficiency: The system defines whether new cryptocurrency units can be created. If new cryptocurrency units can be created, the system defines the circumstances of theirorigin and how to determine the ownership of thesenew units.
- Ownership: Ownership of cryptocurrency units can be proved exclusively cryptographically.
- Accuracy: The system allows transactions to be performed in which ownership of the cryptographic units is changed. A transaction statement can only be issued by an entityproving the current ownership of these units.
- Decision making: If two different instructions for changing the ownership of the same cryptographic units are simultaneously entered,the system performs at mostone of them

Effects of cryptography on modern economy

Markets are dirty. But this doesn't change the fact that cryptocurrencies are here to stayand here to change the world. This is already happening. People all over the world buyBitcoin to protect themselves against the devaluation of their nationalcurrency.

Mostly in Asia, a vivid market for Bitcoin remittance has emerged, and the Bitcoinusing darknets of cybercrime are flourishing. More and more companies discover the power of Smart Contracts or token on Ethereum, the first real-world application of blockchain technologies emerge.

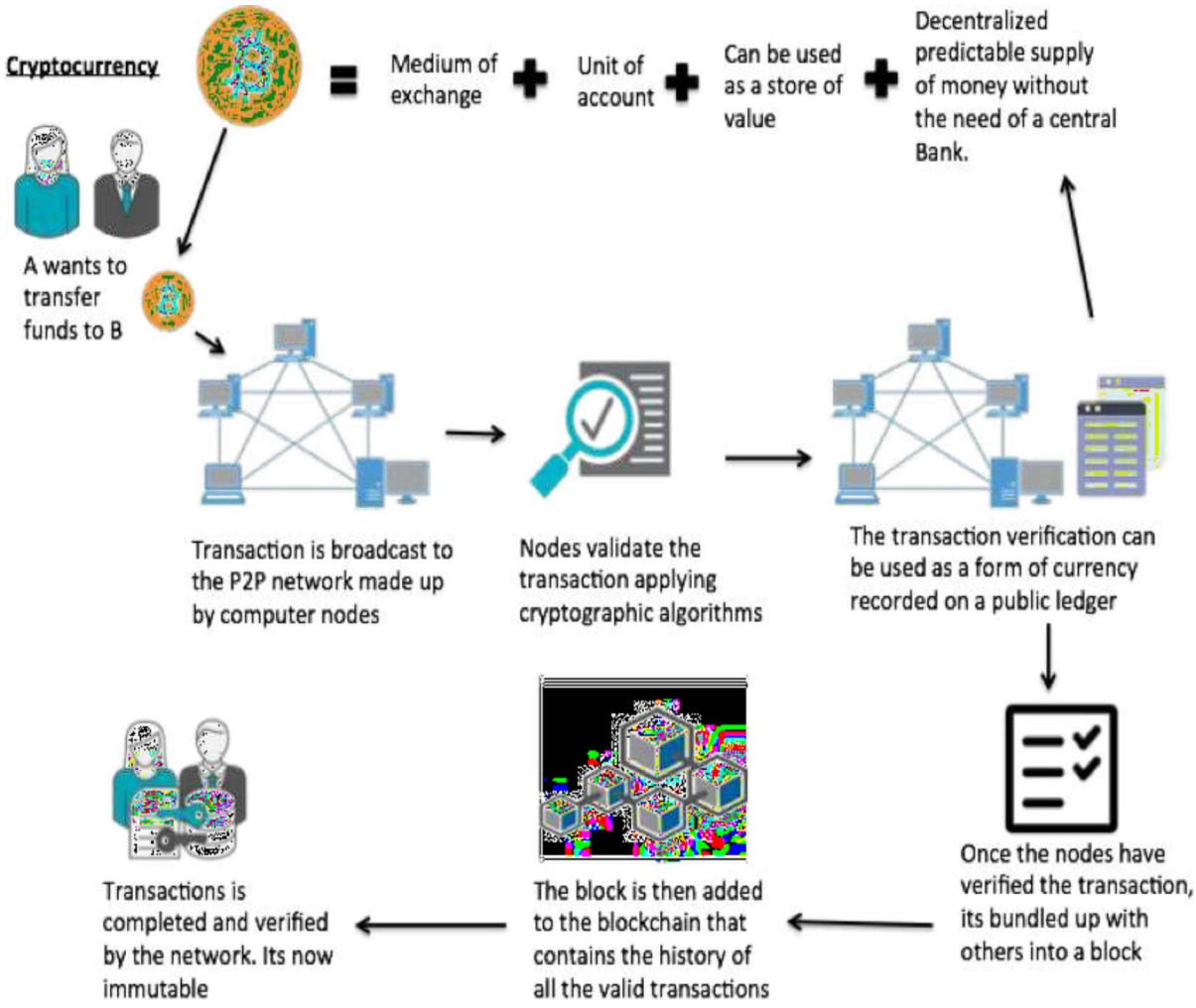

Fig 1 A cryptocurrency model

Decentralization and Blockchain:

- Unlike traditional fiat currencies (such as the US dollar), cryptocurrencies operate decentralized networks.
- The backbone of most cryptocurrencies is the blockchain, a distributed ledger enforcedby a network of computers.
- Transactions are added to the blockchain, creating an immutable record.

Mining and New Coin Creation:

- Mining is the process by which new coins are created and transactions are validated.

- Miners solve complex mathematical puzzles to secure the network and earn rewards inthe form of cryptocurrency.

Digital Wallets and Public Addresses:

- To use cryptocurrency, you need a digital wallet to store your coins securely.
- Wallets generate unique public addresses for receiving funds.

Getting Cryptocurrency:

You can acquire cryptocurrency by:

- Mining: Participating in the network's validation process.
- Trading goods and services: Accepting crypto as payment.
- Buying via brokers and exchanges: Using dollars or other cryptocurrencies.

Types of Cryptocurrencies:

- Bitcoin (BTC): The pioneer and most well-known cryptocurrency.
- Ethereum (ETH): A platform for decentralized applications (DApps) and smartcontracts.
- BNB, Solana, Ripple, and stablecoins are other examples.

Security and Transparency:

- Cryptography ensures security and prevents counterfeiting.
- Transactions are transparently recorded on the blockchain.

#	Name	Market Cap	Price
1	Bitcoin	$289,506,664,615	$17,291.80
2	Ethereum	$64,024,239,344	$664.50
3	Ripple	$31,245,754,581	$0.806568
4	Bitcoin Cash	$30,225,559,633	$1,793.13
5	Litecoin	$14,753,245,951	$271.64
6	IOTA	$10,643,071,611	$3.83
7	Dash	$6,930,780,045	$893.83
8	Cardano	$5,452,099,955	$0.210286
9	NEM	$5,116,022,999	$0.568447
10	Bitcoin Gold	$4,955,520,297	$296.61

Fig 2 Prices of cryptocurrency product

2. BLOCKCHAIN- THE AR CHITECT OFCRYPTOCURRENCY

Introduction

What is blockchain?

Blockchains are secure by design and are an example of a distributed computing system with high Byzantine fault tolerance. Decentralized consensus has therefore been achieved with a blockchain. It solves the double spending problem without the need of a trusted authority or centralserver.

As long as a transaction is unconfirmed, it is pending and can be forged.

When a transaction is confirmed, it is set in stone. It is no longer forgeable, it can"tbe reversed, it is part of an immutable record of historical transactions: of the so- called blockchain.

Why do we need blockchain?Features of blockchain:

- The validity of each cryptocurrency's coins is provided by a blockchain.
- A blockchain is a continuously growing list of records, called *blocks*, which are linked and secured using cryptography. Each block typically contains a hash pointer as a link to a previous block, a timestamp and transaction data.
- By design, blockchains are inherently resistant to modification of the data. It is "an open, distributed ledger that can record transactions between two partiesefficiently and in a verifiable and permanent way".

Nodes within a P2P Network:

- A blockchain network consists of nodes, which can be users or computers. Each nodemaintains a complete copy of the blockchain ledger.
- These nodes collaborate in a peer-to-peer (P2P) network, eliminating the need for acentral server.

Blocks:

- A block is a data structure that contains a set of transactions.
- Each block includes:
  - Cryptographic hash of the previous block (linking blocks together).
  - Timestamp indicating when the block was created.

- Transaction data (records, information, etc.).

Transactions within the Ledger:

- Transactions are the smallest building blocks of a blockchain system.
- They represent actions such as transferring cryptocurrency, recording ownership, orexecuting smart contracts.

Validation Process: Mining:

- The validation process involves mining.
- Miners compete to solve complex mathematical puzzles to validate transactions andcreate new blocks.
- Once validated, the block is added to the blockchain.

Consensus Mechanisms:

- Proof-of-Work (PoW): Used by Bitcoin, miners prove their computational effort tovalidate transactions.
- Other consensus mechanisms include Proof-of-Stake (PoS), Delegated Proof-of-Stake(DPoS), and more.

Benefits of Blockchain Architecture:

- Decentralization: No central authority controls the blockchain, enhancing transparencyand trust.
- Security: Cryptography ensures data integrity and prevents tampering.
- Efficiency: Streamlined processes and reduced intermediaries.
- Applications: Beyond cryptocurrencies, blockchain is used for digital notary, smartcontracts, and more.

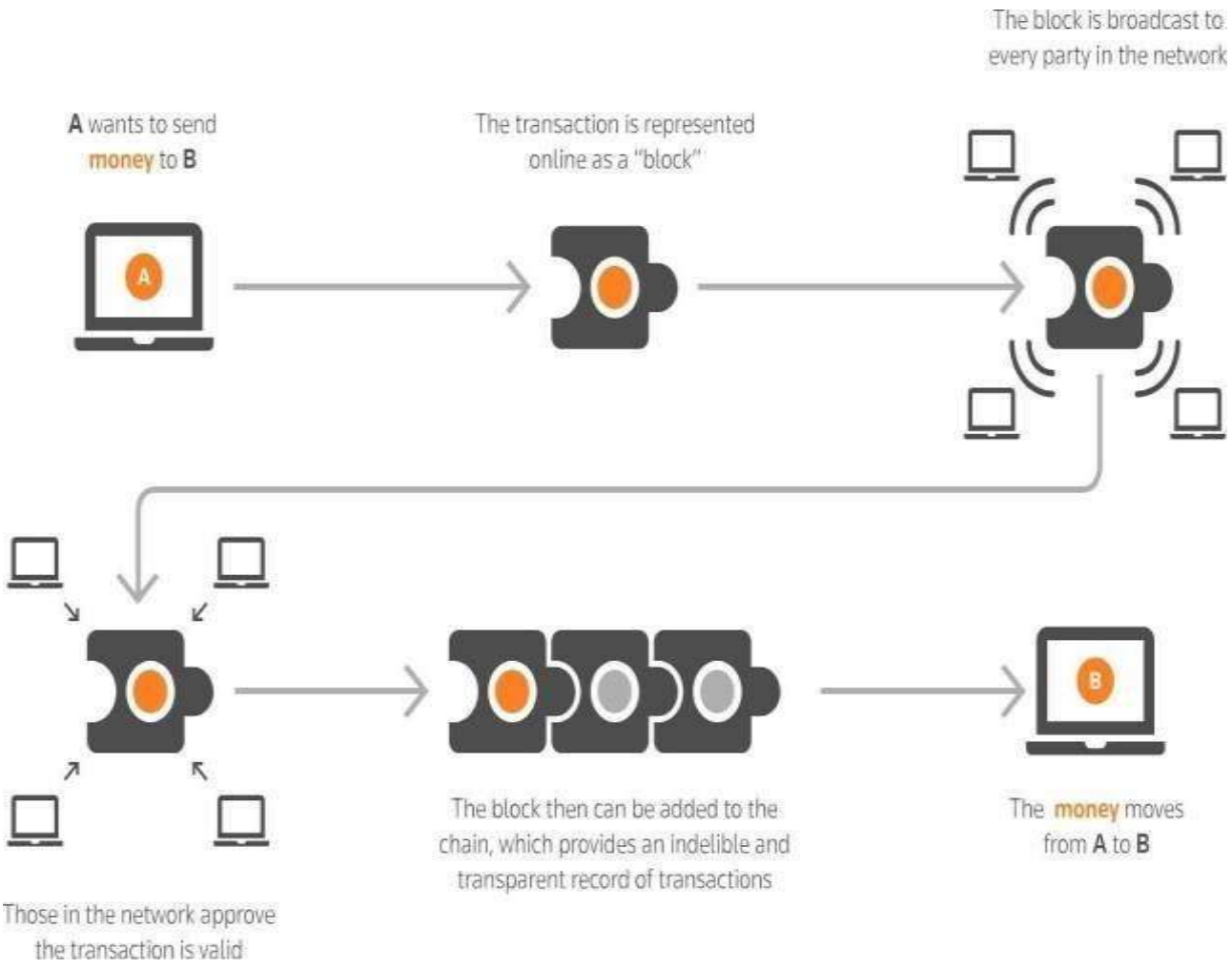

Fig 3 Block diagram of blockchain

3. CRYPTOCURRENCY AND ITS PROPERTIES

Transactional propertiesIrreversible:

After confirmation, a transaction can't be reversed. By nobody. And nobody means nobody.Not you, not your bank, not the president of the United States, notSatoshi, not your miner.

Nobody. If you send money, you send it. Period. No onecan help you, if you sent your funds toa scammer or if a hacker stole them from your computer. There is no safety net.

Pseudonymous:

Neither transactions nor accounts are connected to real-world identities. You receive Bitcoins on so- called addresses, which are randomly seeming chains of around 30 characters. While it is usually possible to analyze the transaction flow,it is not necessarily possible to connect the real-world identity of users with thoseaddresses.

Fast and global:

Transaction is propagated nearly instantly in the network and are confirmed in acouple of minutes. Since they happen in a global network of computers, they are completely indifferentof your physical location. It doesn't matter if I send Bitcoin to my neighbor or to someone onthe other side of the world.

Secure:

Cryptocurrency funds are locked in a public key cryptography system. Only the owner of the private key can send cryptocurrency. Strong cryptography and the magic of big numbers makesit impossible to break this scheme. A Bitcoin address is more secure than Fort Knox.

Permissionless:

You don't have to ask anybody to use cryptocurrency. It's just a software that everybody can download for free. After you installed it, you can receive and sendBitcoins or other cryptocurrencies. No one can prevent you. There is no gatekeeper.

Monetary properties:

Controlled supply:

Most cryptocurrencies limit the supply of the tokens. In Bitcoin, the supply decreases in timeand will reach its final number somewhere in around 2140. All cryptocurrencies control the supply of the token by a schedule written in the code.This means the monetary supply of a cryptocurrency in every given moment in the future can roughly be calculated today. There isno surprise.

No debt but bearer:

The Fiat-money on your bank account is created by debt, and the numbers, yousee on your ledger represent nothing but debts. It's a system of IOU. Cryptocurrencies don't represent debts. They just represent themselves. They are money as hard as coins of gold.

Cryptocurrency Exchange

Cryptocurrency exchanges or digital currency exchanges (DCE) are businesses that allow customers to trade cryptocurrencies or digital currencies for other assets, such as conventional fiat money, or different digital currencies. They canbe market makers that typically take the bid/ask spreads as transaction commissions for their services or simply charge fees as a matching platform

Fig 4 Block diagram of cryptocurrency exchange

4. CRYPTOCURRENCY- ITS MERITS AND DEMERITS

Merits:

No need for banks

It's thought that around four billion people worldwide have no bank account, seemingly showing that there would be a demand for a currency that can be accessed easily online. The lack of a need for banks results in decentralization and allows individuals to have full controlover their money, cutting out the third party.

Digital e-cash

With the growth of the digital world, having an easy way to pay online is becoming more and more essential. Cryptocurrency makes this possible, which also greatly increases the speed of transactions. Rather than waiting for several working days for money to process – as used to bethe case with cheques – funds can be sent in just 10 minutes.

Inflation Protection:

Unlike traditional fiat currencies, cryptocurrencies are not subject to inflation. Their value remains relatively stable, making them a potential hedge against currency devaluation1.

Transactional Speed:

Cryptocurrency transactions can occur swiftly and directly between parties without intermediaries like banks. This efficiency is especially beneficial for cross-border transfers1.

Cost-Effective Transactions:

Cryptocurrencies often have lower transaction fees compared to traditional banking systems.This cost-effectiveness appeals to users seeking efficient payment methods1.

Decentralization:

Cryptocurrencies operate on decentralized networks (such as blockchain), which means they are not controlled by any central authority. This decentralization enhances security and reducesthe risk of government interventions1.

Diversity:

The crypto market offers a wide variety of coins and tokens, allowing investors to choose based on their preferences, risk tolerance, and investment goals1.

Accessibility:

Anyone with an internet connection can participate in the cryptocurrency market. This inclusivity democratizes financial access globally1.

Safety and Security:

Cryptocurrencies use cryptographic techniques to secure transactions. Once confirmed, transactions are irreversible, reducing fraud risks1.

Transparent:

Blockchain technology ensures transparency by recording all transactions on a public ledger.Users can verify and trace transactions easily1.

Demerits:

Lack of real-world use

Although cryptocurrency's usage is increasing, it lacks application in the real world. There arestill relatively few businesses who accept Bitcoin, for example.

Lack of transparency and security

A lack of information and understanding about cryptocurrency transactions makes it difficult for governments to regulate or tax, leading to a host of criminal activity and problems for investors. Fears of exchanges being hacked are also a real problem and issues with wallets cause a lot of uncertainty.

Lack of Awareness/Knowledge:

Many people are still unaware of digital currencies like Bitcoin. Their limited understanding ofcryptocurrency can lead to misconceptions and uninformed decisions.

Use of Complex Techniques:

Cryptocurrencies operate on intricate cryptographic systems. Understanding these technologies canbe challenging for the average user.

High Volatility:

The value of cryptocurrencies can fluctuate dramatically within short time frames. This volatilityposes risks for investors and makes it difficult to predict their future worth.

Not Universally Accepted:

Unlike traditional fiat currencies, cryptocurrencies are not universally accepted. Their limitedadoption restricts their use for everyday transactions.

Victim of Theft and Scams:

The decentralized nature of cryptocurrencies makes them susceptible to theft, hacking, and fraudulentschemes. Once funds are lost, recovery is often impossible.

Irreversible Transactions:

Unlike credit card payments, cryptocurrency transactions are irreversible. If you send funds to thewrong address or fall victim to a scam, there's no recourse.

Black Market Usage:

Cryptocurrencies have been associated with illegal activities due to their anonymity. Criminals mayuse them for money laundering, tax evasion, and other illicit purposes.

Energy Consumption:

The process of mining cryptocurrencies consumes significant energy resources. This environmentalimpact is a concern for sustainable practices.

Lack of Sovereign Guarantee:

Unlike traditional currencies backed by governments, cryptocurrencies lack any sovereign guaranteeor approval. Their value relies solely on market dynamics.

Regulatory Uncertainty: The regulatory landscape for cryptocurrencies varies globally.Uncertainty about future regulations can affect investor confidence.

Pro's	Con's
Anything of value can be transferred and saved safely and confidentially - without unlawful alteration	Scammers and other seedy characters can use the anonymity to their advantage to do evil
Transactions are verifiable by a vast, peer-to-peer global network	Hacks and manipulation can still occur
Cryptocurrencies are not able to be "frozen" in the case of economic crisis (such as your money in the bank would be)	The majority of governments, offices, retailers, and everyone who deals with money, do not understand, let alone use / accept cryptocurrencies as valid payment.
There will no longer be the need for intermediaries such as banks, lawyers, government, etc.	Many people are currently employed in institutions that serve as intermediaries… there will certainly be a lot of resistance
Transactions are irreversible.	Transactions are irreversible.
1 Bitcoin is (as of this publication) worth $1252 USD, and has increased in value over time	Behind the scenes, there may be trouble with bitcoin, and there are rumors of it splitting into two separate cryptocurrencies

Table 1 Tabular summary of the pros and cons of cryptocurrency

5. CRYPTOCURRENCY PROJECTS

Bitcoin:

The one and only, the first and most famous cryptocurrency. Bitcoin serves as a digital gold standard in the whole cryptocurrency-industry, is used as a global means of payment and is the de-facto currency of cyber-crime like darknet markets or ransomware. After seven years in existence, Bitcoin's price has increased from zero to more than 650 Dollar, and its transaction volume reachedmore than 200.000 daily transactions.

Litecoin:

Litecoin was one of the first cryptocurrencies after Bitcoin and tagged as thesilver to the digital gold bitcoin. Faster than bitcoin, with a larger amount oftoken and a new mining algorithm, Litecoin was a real innovation, perfectly
tailored to be the smaller brother of bitcoin. "It facilitated the emerge of several other cryptocurrencies which used its codebase but made it, even more, lighter". Examples are Dogecoin or Feather coin. It is still actively developed and tradedand is hoarded as a backup ifBitcoin fails.

Monero:

Monero is the most prominent example of the cryptonite algorithm. This algorithm was invented to add the privacy features Bitcoin is missing. If you useBitcoin, every transaction is documented in the blockchain and the trail of transactions can be followed. With the introduction of a concept called ring- signatures, the cryptonite algorithm was able to cut through that trail.

Ripple (XRP):

Ripple aims to revolutionize cross-border payments by enabling fast and low-cost transactions. It collaborates with financial institutions and banks to facilitate international money transfers.

Cardano (ADA):

Cardano focuses on scalability, security, and sustainability. It aims to create a more efficient andsecure blockchain infrastructure for DApps and smart contracts.

Polkadot (DOT):

Polkadot is a multi-chain blockchain platform that allows different blockchains to interoperate. Itaims to enhance scalability, security, and governance.

Chainlink (LINK):

Chainlink provides decentralized oracle services, connecting smart contracts with real-world data. Itensures reliable and tamper-proof data feeds for DApps.

Solana (SOL):

Solana is known for its high throughput and low transaction fees. It aims to support decentralizedapplications and DeFi projects.

Binance Coin (BNB):

BNB is the native token of the Binance exchange. It offers discounts on trading fees and serves as autility token within the Binance ecosystem.

Avalanche (AVAX):

Avalanche focuses on scalability, interoperability, and customizability. It aims to provide a robustplatform for decentralized applications.

Polygon (MATIC):

Formerly Matic Network, Polygon enhances Ethereum scalability by providing layer-2 solutions. Itaims to improve transaction speed and reduce fees.

Sl. No.	Name	Market cap	Price	Availablesupply	Volume	%change
1	Bitcoin	$11382240050	$712.76	15969336 BTC	$67288200	-1.60%
2	Ethereum	$904848975	$10.54	85831133 ETH	$4069260	-1.21%
3	Ripple	$290446848	$0.08	35765131899 XRP	$2386420	0.26%
4	Litecoin	$1804904214	$3.82	48378029 LTC	$2258970	-1.05%
5	Monero	$83466495	$6.27	13311446 XMR	$3134490	5.38%
6	Ethereum classic	$80817441	$0.94	85735486 ETC	$603573	2.21%
7	Dash	$66519213	$9.68	6874532 DASH	$596632	-0.77%
8	Augur	$52038360	$4.73	11000000 REP	$396072	6.38%
9	NEM	$37322520	$0.04	8999999999 XEM	$86817	4.40%
10	Waves	$35727500	$0.35	1000000000 WAVES	$133650	-3.94%
11						

Table 2 stock report on cryptocurrency

Statistics:

While Bitcoin remains by far the most famous cryptocurrency and most other cryptocurrencieshave zero non-speculative impact, investors and users should keep an eye on several cryptocurrencies.

Here we present the most popular cryptocurrencies of today in the above figure.

6. EFFECTS OF CRYPTOCURRENCY ON ECONOMY

Commercial changes due to cryptocurrency:

Lotteries

In December 2017 Gibraltar based gaming operator Lotto land launched the world's first regulated bitcoin lottery offering a 1000 bitcoin jackpot. Players still pay in traditional currencies but can receive their winnings in bitcoin if they choose.

Causing a rise in GPU prices

The sudden increase in cryptocurrency mining has increased the demand of graphics cards (GPU) greatly. Popular favorites of cryptocurrency miners such as Nvidia's GTX 1060and GTX
1070 graphics cards, as well as AMD‟s RX 570 and RX 580 GPUs, have all doubled if not tripled in price – or are out of stock completely. A GTX 1070 Ti which was released at a price of $450 is now being sold for as much as $1100.

Probable fluctuations in currency

While cryptocurrencies are digital currencies that are managed through advanced encryption techniques, many governments have taken a cautious approach toward them, fearing their lack of central control and the effects they could have on financial security. Regulators in several countries have warned against cryptocurrency and some have taken concrete regulatory measures to dissuade users. Additionally, many banks do not offer services for cryptocurrencies and can refuse to offer services to virtual-currency companies. While traditional financial products have strong consumer protections in place, there is no intermediary with the power to limit consumer losses if bitcoins are lost or stolen. One of the features cryptocurrency lacks in comparison to credit cards, for example, is consumer protection against fraud, such as chargebacks.

Regulation and Stability:

A majority of macroeconomists agree that both cryptocurrencies and stablecoins should have a regulated rolein economies. These digital currencies could potentially drive:

- Financial stability: By providing alternative financial systems and reducing reliance ontraditional banks.
- Equity: Enabling broader access to financial services, especially for the unbanked.
- Innovation: Fostering technological advancements in payment systems and financialinfrastructure.
- Market incentives for environmental sustainability: Encouraging eco-friendly practices inthe crypto industry.

Spillover Effects:

- Concerns exist regarding the potential spillover effects of crypto and stablecoins on thefinancial system.
- Regulatory efforts, such as the Markets in Crypto-Assets (MiCA) Regulation in theEuropean Council, aim to address these concerns.

Decision-Making and Projections:

- Policymakers and business leaders need projections to inform decision-making in thisdynamic space.
- Research aims to project economic outcomes based on various regulatory paths.

CONCLUSION

- Cryptocurrencies such as Bitcoin still have number of obstacles before, they couldtotally replace current currency systems.
- No. of users is the biggest challenge to adopt the crypto as universal currency.
- Prices is also one factor in adoption, as prices of cryptocurrencies varies time to time.
- To adopt it one only need the internet connection, not dependent on institutions such asbanks.
- In the next 10-15 years Cryptocurrencies will have the potential to replace the Govt.backed fiat currencies.
- At present roughly 3-5 percent peoples only use cryptocurrencies.
- Pi network will boost the adoption of cryptocurrencies, due to its low prices andtechnology behind it.

REFERENCES

[1] https://www.kaspersky.com/resource-center/definitions/what-is-cryptocurrency.

[2] https://indianexpress.com/article/explained/explained-what-does-rbis-latest-circular-on-cryptocurrencies-mean-7339651/

[3] https://www.indiatoday.in/business/story/rbi-s-clarification-on-cryptocurrency-what-it-means-for- cryptocurrency-trade-in-india-1809419-2021-06-01

[4] https://www.coindesk.com/learn/what-is-cryptocurrency/

[5] https://www.investopedia.com/terms/c/central-bank-digital-currency-cbdc.asp

[5] https://cointelegraph.com/learn/what-are-cbdcs-a-beginners-guide-to-central-bank-digital-currencies

[6] https://cryptocurrencyfacts.com/

[7] https://en.wikipedia.org/wiki/Cryptocurrency