A DETAILED ANALYSIS OF CRYPTO-BAN IN NEPAL

Written by ***Anurag Aryal*, Ashish Pandey**, Pratistha Ghimire***, Abishekh Dhakal****, Karigya Joshi#, Ankit Gautam^ & Srijan Sapkota^^***

** High School Graduate, Tilottama Secondary School, Butwal, Nepal*

*** High School Graduate, Tilottama Secondary School, Butwal, Nepal*

**** High School Graduate, Xavier Academy, Kathmandu, Nepal*

***** High School Graduate, Nist National School of Sciences, Kathmandu, Nepal*

 # High School Graduate, Valmiki Shiksha Sadan Secondary School, Bharatpur, Nepal

^ High School Graduate, Tilottama Secondary School, Butwal, Nepal

^^High School Graduate, Aroma College of Applied Science and Management, Bharatpur, Nepal

ABSTRACT

General Background and Our Motivation

Digitalization has engulfed every corner and domain of the globe, and currencies are no exception. As computer science enthusiasts, we were, are, and will always be enthralled by the prospects of digitalized currency. Cryptocurrencies are globally considered the future of financial transactions because of the leverage they offer in the form of decentralized and independent transactions. But in August 2017, the government of Nepal declared a ban on cryptocurrencies. It was shocking news for us and we wanted to understand why such a harsh decision was taken.

Before starting to work on this research, we searched comprehensively on the internet to see whether there were any research papers were associated with this subject matter. But, we couldn't find any. Therefore, we decided to work on this paper. With this research, we aspire to elucidate the rationale behind the ban of cryptocurrencies by the Nepal Rastra Bank (NRB), the central bank of Nepal. We would attest to our devotion to this research by stating that we

allocated 1 hour every day in the last 4 weeks to make this paper as accurate and efficient as possible.

Our Data Collection Approach

The information used in this research assessment is entirely secondary and was derived from various online articles and journals. We have taken into account those facts, carefully examined them, and tried to link several elements that are either directly or indirectly responsible for the ban of cryptocurrency in our country.

INTRODUCTION

Monetary transactions have come a long way, starting from the barter system to paper money to today's digital currencies. Paper money, which was widely recognized and used a couple of years ago, is now only used in 2% of transactions as digital currencies are taking over the international market. The most popular digital currency nowadays is cryptocurrency, thanks to its flexibility and advanced security. A cryptocurrency is a unit of currency represented by an encrypted data string. The transactions take place on a computer network that is not under the control of a bank or a government. Cryptocurrencies are becoming increasingly popular because they offer a platform where tax can be avoided.

A peer-to-peer network called a blockchain is used to monitor cryptocurrency. This peer-to-peer network allows for connections between individuals without the intervention of a third party like a bank or government. The blockchain assures the legitimacy of each crypto-coin. Each block consists of transaction information, a timestamp, and a cryptographic hash of the previous block. The cryptographic hash function offers the advanced security that we previously mentioned. It accepts an arbitrary quantity of data as input and gives a fixed-size encrypted text called “hash value” as output. The encrypted text can then be stored in place of the password and used later to confirm the user's identity. It is a one-way function that resists collisions and is unpredictable. Since hackers must first decipher the hash values to exploit them, the currency is safer.

There are two ways to earn cryptocurrency. One way is to purchase it from the broker. Another option is mining. When a new crypto transaction is conducted, it is sent to the miners (Crypto

users) for verification in the crypto mining process. A mathematical proof of work is required for verification and it involves billions of calculations per second. The transaction is verified and added to the blockchain once the complex mathematical task is solved, and the miner who solved it first is rewarded with a new cryptocurrency. The mining process is expensive because it needs strong computers, a high-tech power supply, and a sophisticated cooling system. Bitcoin miners are actual people who own cutting-edge computing hardware. While gold and silver miners use shovels and bulldozers for mining, bitcoin miners use powerful computers, hence the name metaphorically. Mining is the fundamental block of existence and relevance for cryptocurrencies. Since cryptocurrencies are essentially digital records, there is a possibility of copying, counterfeiting, or double spending the same coin. This issue is resolved via mining, as it makes this process very costly and resource-intensive.

Different cryptocurrencies are available in the market. But, the most popular one is Bitcoin. One important thing to understand is that the supply of cryptocurrencies is restricted by either setting a definite limit on how many can exist or through minting and burning. For instance, there cannot be more than 21 million bitcoins. A limit is imposed for bitcoins to prevent dramatic price fluctuations, just like regular paper currency, which the government cannot arbitrarily print more of. But cryptocurrencies such as Ethereum are minted and burnt so that value and inflation can be controlled. Minting refers to the creation of new coins through the verification of transactions. Burning cryptocurrency refers to sending the coin to a location in the blockchain from where it cannot be regained. A specific quantity of Ethereum is taken as a base fee with each transaction and burned. Burning is done to a significant extent time and again.

HISTORICAL BACKGROUND

American cryptographer David Chaum introduced Digicash, an anonymous cryptographic electronic currency, in 1995. It was an early example of a cryptographic electronic payment that required user software to withdraw from a bank and certain encryption keys to transfer it to a receiver. BitGold was later created by Nick Szabo and is considered a precursor of bitcoin. Users had to employ computer resources to resolve cryptographic puzzles; those who

succeeded were rewarded. Something that resembles Bitcoin might have been created by combining the ideas of Chaum and Szabo.

On October 31, 2008, an unidentified author going by the name of Satoshi Nakamoto published a paper, titled "Bitcoin-A Peer to Peer Electronic Cash System," outlining how the Bitcoin blockchain network functions. And, on January 3, 2009, he mined the very first block of the Bitcoin network. Then, the first real-world use of cryptocurrency was seen in 2009 with bitcoin.

MATHEMATICAL MODELLING OF BLOCKCHAIN

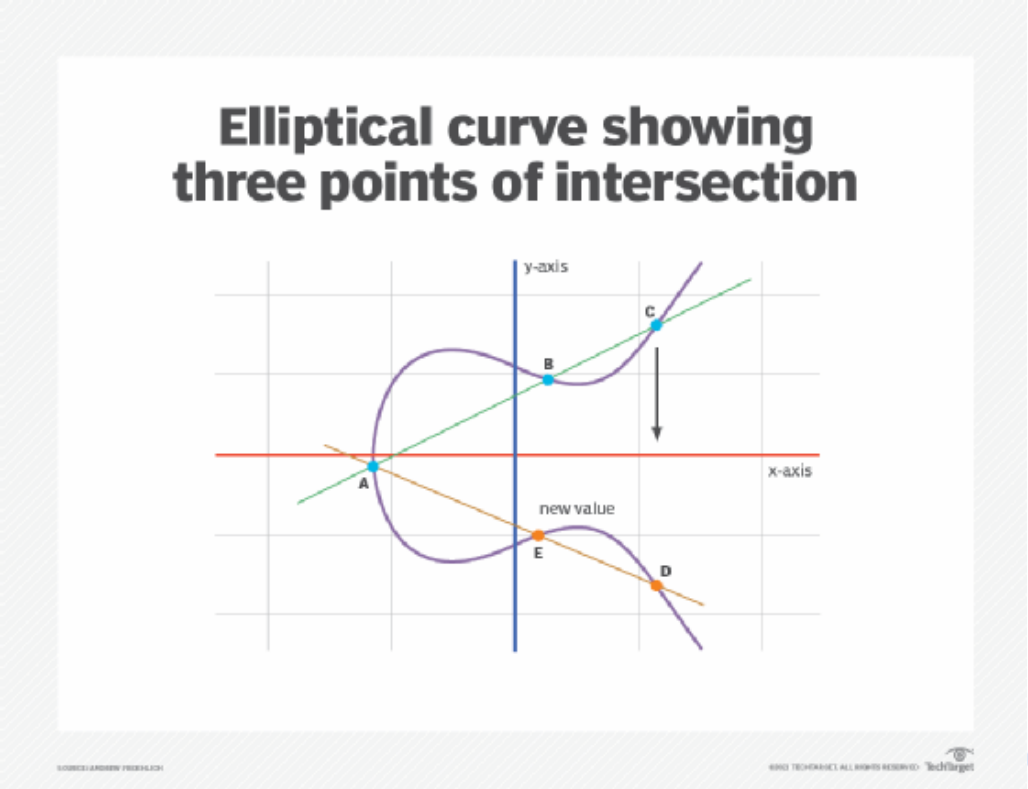
As previously mentioned, complex mathematical calculations and models are incorporated for transactions using cryptocurrencies. These concepts are crucial for smooth functioning. Some of the mathematical tools for the effective transaction of bitcoin are explained below:

Elliptical Curve Cryptography (ECC)

ECC is the process of creating public and private key pairs across a finite field using elliptical curves. The public key is utilized while sending cryptocurrency into the wallet of the buyer during a transaction. On the other hand, private key.is employed to validate transactions and demonstrate ownership over a blockchain address.

It has an elliptical curve form, which is shown below:

$y^2=ax^3+bx^2+cx+d.$

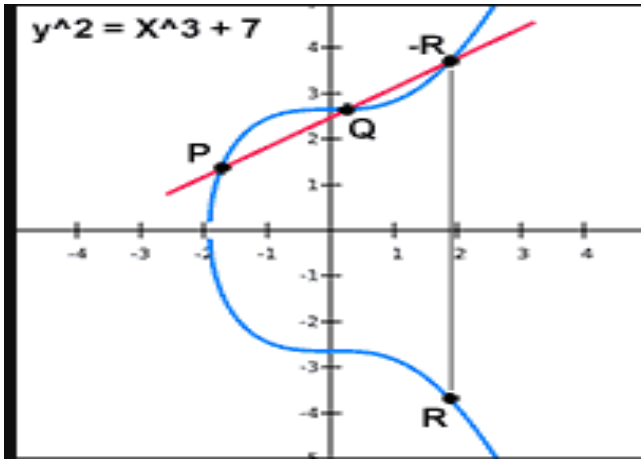


Courtesy: techtarget.com

The fact that it is derived within ECC over a finite field ensures that both the x and y axes have a limit. Utilizing the characteristics of these curves enables the creation of two connection points on the curve, one of which is simple to compute and the other of which is difficult to compute. This is known as asymmetric cryptography and enables the separation of private and public keys.

The geometry of the Bitcoin elliptic curve is:

$y^2 = x^3+d$



Courtesy: Steemit

The value of the constant d, in this case, is 7 mod 1.1581077. This curve, known as secp256k1, is a Kobiltz curve. Secp256k1 was built in a non-random manner as opposed to typical elliptical curves, which have a random structure, to aid in efficient computing. Public and private keys that enable users to accept and spend bitcoin are created using Secp256k1. The public key is accessible to the whole public, whereas a user's private key is only known to them.

RESULTS

Following extensive research and examination of the data on the internet, we have identified some likely causes behind the government of Nepal's decision to ban cryptocurrencies. These reasons are listed below:

1. ***National Laws and Acts***

   Despite the popularity of cryptocurrencies in the modern world, Nepal has not yet officially accepted them for financial transactions. Although the Constitution doesn't explicitly define cryptocurrency, some laws have been made that have an indirect impact on it and its ban. The laws and acts that prohibit the use of cryptocurrency in our country are mentioned below:

- Act Restricting Investment Abroad, 1964 (was made with the National Panchayat's approval and the advice of His Majesty King Mahendra Bir Bikram Shah dev)
- Foreign Exchange Regulation Act, 1962
- Foreign Investment and Transfer of Technology Act (FITTA), 2019 (although this act was formulated after the declaration of the crypto-ban, this act has been strongly advocating for the prohibition of cryptocurrencies since its enactment)

Nepal's 1964 Act on Restricting Investment Abroad states that Nepalese citizens are not allowed to invest abroad, which includes crypto investment too. The Foreign Exchange Regulation Act and FITTA aim to promote the use of foreign exchange for payments, foreign investment, and technology transfer. They have five different scopes. The major setbacks for crypto transactions and regulation are the scopes of "Regulations of foreign-related transactions" and "Use of foreign exchange investment and technology transfer." They essentially support the ban on cryptocurrencies and their uses.

2. Defrauding

No one can access the identity of a buyer or seller because of the decentralized system and uncompromising anonymity provided by cryptocurrency. Criminals may commit horrible crimes like money laundering, terrorism, and drug trafficking without ever being caught. Many governments, including the government of Nepal, believe that the use of cryptocurrencies will cause an increase in the number of these heinous crimes. Additionally, it is believed that cryptocurrencies expose investors to a variety of frauds and scams. One such issue that can cause some investors to lose their hard-earned money is misleading advertising. Our policymakers might have also cited this reasoning while discussing the ban on cryptocurrencies. If they had banned crypto based on this reasoning, we can't be too skeptical about the rationale of their decision as many such cases of defrauding have happened in the last couple of years. One such case is mentioned below:

In October 2021, the cybercrime bureau of the Hyderabad police department received a complaint from B. Kiran of Ghatkesar, who claimed that he lost Rs 86 lakh in the

hope of receiving big returns after clicking on a link for an online investment scheme sent by the accused. The victim clicked on the link and later sent money to different bank accounts as instructed by the accused. Later, he discovered that he was unable to receive the promised funds from the accused. Police detained three Siliguri residents after receiving his allegation and discovered that Depu Mandal, a Nepali, was the main suspect. Although the police had started looking for Depu, they learned that three other Nepalese—Gopal, Sushil, and Nima—who were in Hyderabad and were setting up a call center to deceive people by pitching them false investment plans—were also involved. "Depu made bogus ID credentials and gave them to the suspects who had been imprisoned. He used them to open bank accounts and get SIM cards. According to Rachakonda police, a check of a messaging app on the accused's phone revealed that the fraud's gains were routed to China via a cryptocurrency exchange.

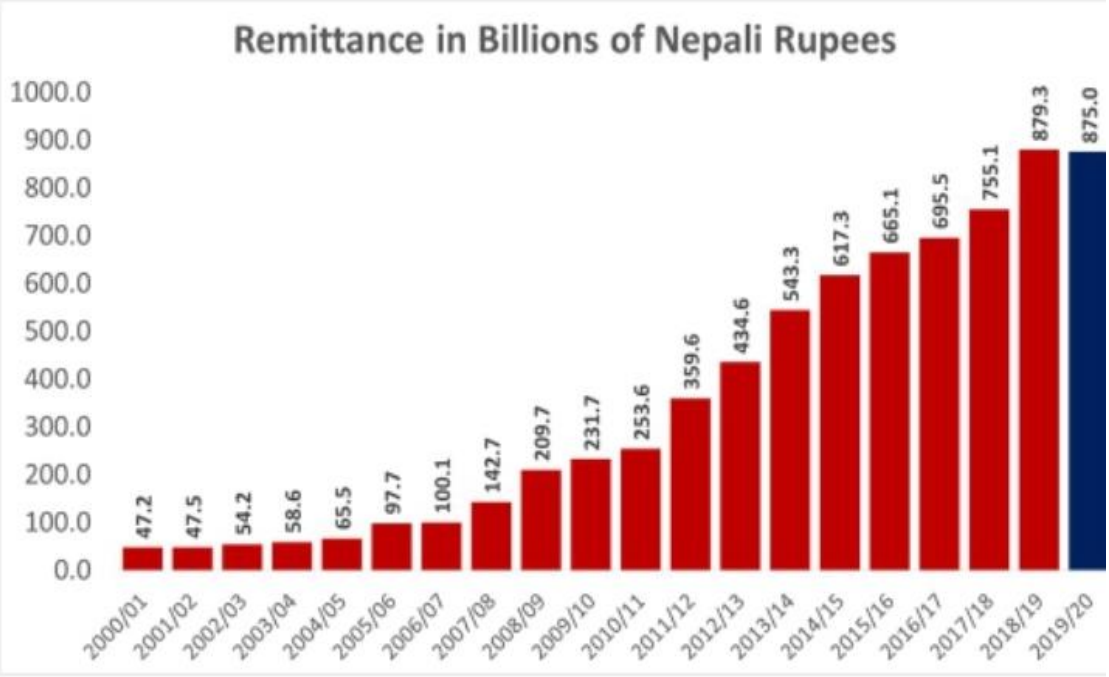
3. ***Lack of Regulation***

There is no regulation of the value of cryptocurrencies. The value of a particular cryptocurrency would substantially drop if a sizable investor group decided to stop using it and sell it, which would have an immediate impact on millions of users. One such incident was observed in January 2022. Over $600 billion in market value was lost by Bitcoin since its November 2021 peak, and over $1 trillion was lost by the whole crypto market in the first month of 2022. This daunting scenario is unacceptable for a country with a fragile economy like Nepal. This might be one of the most important reasons behind the crypto-ban in Nepal.

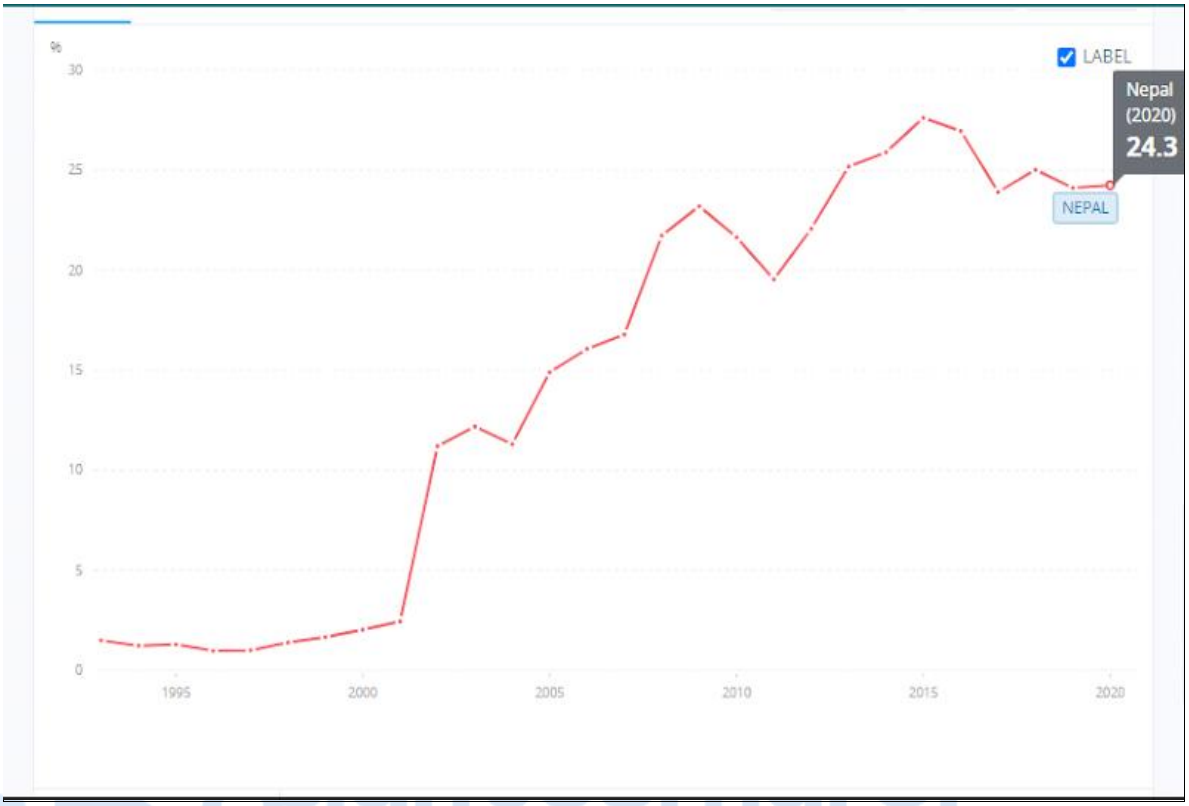
4. ***Effects on Remittance***

Remittances play a huge role in the Nepalese economy, accounting for about a quarter of the country's GDP. The Nepalese economy might crash if people start sending money in the form of cryptocurrency from abroad. The Nepalese government lacks the technological means to track the crypto transactions that are carried out online. As a result, there is less money to be taxed, which could eventually lead to the collapse of the national economy. No evidence supports the fact that cryptocurrencies result in a decrease in remittances. However, the income generated from remittance has been decreasing in the last couple of years and it is claimed that the number of crypto-

investors has been increasing throughout this period. In just the current fiscal year 2021–2022, remittance inflows dropped by 7.3%. Even Mr. Janardhan Sharma, the former finance minister of Nepal, once claimed that the use of cryptocurrencies is responsible for the current decline in remittances. And, recent statistics about the income generated from remittances also portray this relation.



ISSN 2582 8088
Volume 3 Issue 4 [July August 2022]



Probably, policymakers saw this coming and enacted the infamous crypto-ban. Needless to say, this situation might have been worse if cryptocurrencies were legalized.

5. ***Impacts on the Foreign Reserve***

Cryptocurrency has twofold effects on a country's foreign exchange reserves. First, the central bank will have to buy cryptocurrencies to maintain its foreign exchange reserves if a significant portion of a country's residents purchase them. As a result, other countries access to foreign currency would be reduced, which could have an impact on trade balances. Second, if a country's central bank starts to recognize cryptocurrencies as a component of its foreign reserve assets, this might boost demand for the currency and cause it to appreciate against other currencies. This will negatively impact the country’s financial status. This could be considered one of the most prominent reasons behind the ban of cryptocurrencies in Nepal.

SUPPLEMENTARY INFORMATION

1. ***Crypto-Ban Declaration Issued by NRB In 2017***

नेपाल राष्ट्र बैंक, केन्द्रीय कार्यालय
विदेशी विनिमय व्यवस्थापन विभागको
Bitcoin कारोवार गैरकानुनी रहेको बारेको सूचना

नेपाल राष्ट्र बैंक ऐन, २०५८ र विदेशी विनिमय (नियमित गर्ने) ऐन, २०१९ बमोजिम यस बैंकबाट इजाजतपत्र लिएर मात्र विदेशी विनिमयको कारोबार गर्न सक्ने स्पष्ट कानुनी व्यवस्था रहेको र हालसम्म नेपालमा Bitcoin लाई मुद्राको रुपमा कानुनी मान्यता प्राप्त नभएको अवस्थामा यदाकदा केही व्यक्तिहरुले इन्टरनेटको माध्यमबाट Bitcoin सम्बन्धी कारोवार गरिरहेको भन्ने बुझिन आएकोले Bitcoin सम्बन्धी कारोबार नेपालमा पूर्णरुपमा गैरकानुनी रहेको व्यहोरा जानकारी गराउँदै कसैले पनि सो सम्बन्धी कारोवार नगर्न नगराउनुहुन सर्वसाधारणको जानकारीको लागि यो सूचना प्रकाशन गरिएको छ ।

कार्यकारी निर्देशक
विदेशी विनिमय व्यवस्थापन विभाग

मिति : २०७४।४।२९

2. ***Nepal to Launch its own Cryptocurrency***

To permit the monetary authority to issue a digital version of the nation's fiat currency, the Nepalese rupee, the Nepal Rastra Bank (NRB) is prepared to amend the legislation defining its rights and obligations. The information comes after a study that concluded that a central bank digital currency (CBDC) initiative is feasible. The government of Nepal seems to have finally accepted that cryptocurrencies hold the future of financial transactions. However, Nepal can't rely on the cryptocurrencies available in the market because they create many issues, as mentioned above. If Nepal can maintain regulation, stability, and minimum validation and ensure that no taxes are waived and it has no consequences on the foreign reserves, issuing a national digital currency might be a great initiative.

CONCLUSION

In this research, we carefully assessed the reasoning behind the Nepal government's decision to ban cryptocurrencies in Nepal. Despite the prohibition, it is reported that many people in Nepal engage in crypto transactions daily. Nepalese people need to understand that the policymakers made such a decision after a thorough analysis. As we mentioned, it could lead to many daunting circumstances. So, they should respect the law and stop committing crimes. It is also noteworthy that government officials are trying their absolute best to incorporate a digital innovation referred to as the future of monetary transactions in Nepal. But, it will take time considering the financial, human, and infrastructural resources we have. Until then, we urge everyone to respect our policymakers' decisions and refrain from investing in such currencies.

FUNDING

This research received no external funding.

CONFLICT OF INTEREST

None declared.

REFERENCES

- Vivien Lee and David Wessel, *Digital currencies: Five big implications for central banks*, BROOKLINGS.EDU (March 09, 2022, 03:47 AM), https://www.brookings.edu/blog/up-front/2018/05/21/digital-currencies-five-big-implications-for-central-banks/.

- Wikipedia contributors, *Foreign exchange reserves*, WIKIPEDIA, THE FREE ENCYCLOPEDIA (26 July 2022, 00:58 UTC), https://en.wikipedia.org/w/index.php?title=Foreign_exchange_reserves&oldid=1100454485

- Central Bank of Belize, *Financial Infrastructure*, https://www.centralbank.org.bz/financial-system/financial-infrastructure.

- Hannah Smith,, *Bitcoin crash: what's behind crypto collapse?* THE TIMES (July 4, 2022, 07:47 AM), https://www.thetimes.co.uk/money-mentor/article/is-bitcoin-crash-coming/.

- Wikipedia contributors, 'Cryptocurrency', WIKIPEDIA, THE FREE ENCYCLOPEDIA *(*August 27, 2022, 04:22 UTC), https://en.wikipedia.org/w/index.php?title=Cryptocurrency&oldid=1106916101.

- Kaspersky, *What is cryptocurrency and how does it work*?, KASPERSKY(n.d.), https://www.kaspersky.com/resource-center/definitions/what-is-cryptocurrency

- Tara Annison, *The Maths Behind the Bitcoin Blockchain*, LINKEDIN (July 2, 2018),
- https://www.google.com.np/url?sa=t&source=web&rct=j&url=https://www.linkedin.com/pulse/maths-behind-bitcoin-blockchain-tara-annison&ved=2ahUKEwittoy1xMj4AhUR-DgGHV3rCyMQjjh6BAgTEAE&usg=AOvVaw30cSlmT8LtYJ5Vc8lcKYa6
- Alex Gailey, *Should You Buy the Crypto Dip While Bitcoin and Ethereum Prices Are Down?*, NEXTADVISOR (August 19, 2022),
- https://time.com/nextadvisor/investing/cryptocurrency/should-i-buy-crypto-dip/#:~:text=Bitcoin%2C%20ethereum%2C%20and%20crypto%20prices,interest%20rates%2C%20and%20recession%20fears.
- Euny Hong, *How Does Bitcoin Mining Work?*, INVESTOPEDIA (May 5, 2022), https://www.investopedia.com/tech/how-does-bitcoin-mining-work/#:~:text=Why%20Do%20Bitcoins%20Need%20to,otherwise%20%22hack%22%20the%20network.
- Mint, *8 Pros and Cons of Bitcoin*, INTUIT MINT LIFE(n.d.), https://mint.intuit.com/blog/investments/pros-and-cons-of-bitcoin/
- Prithvi Man Shrestha, *Central bank sees capital flight risk in illegal investments in cryptocurrencies*, THE KATHMANDU POST (February 9, 2022), https://kathmandupost.com/national/2022/02/09/central-bank-sees-capital-flight-risk-in-illegal-investments-in-cryptocurrencies
- Winston Moore and Jeremy Stephen, *Should cryptocurrencies be included in the portfolio of international reserves held by central banks?*, COGENT ECONOMICS AND FINANCE (February 16, 2016), https://www.tandfonline.com/doi/full/10.1080/23322039.2016.1147119
- Evan Jones,*A Brief History of Cryptocurrency*, GANDI SAS(Jul 25,2022,11 A.M.), https://www.cryptovantage.com/guides/a-brief-history-of-cryptocurrency/
- WIKIPEDIA THE FREE ENCYCLOPEDIA,"*Bitcoin*",WIKIPEDIA FOUNDATION,INC.(Jul 27,2022,9:05 P.M.), https://en.wikipedia.org/wiki/Bitcoin
- Adam Hayes,*Blockchain Facts:What is it,How it works,and How it can be used*,MARKMONITOR,INC.(Jun 15,2022,8 A.M.), https://www.investopedia.com/terms/b/blockchain.asp

- Prithvi Man Shrestha,*Central Bank sees capital flight risk in illegal investments in cryptocurrencies,*THE KATHMANDU POST(Aug 20,2022,7:20 P.M.), https://kathmandupost.com/national/2022/02/09/central-bank-sees-capital-flight-risk-in-illegal-investments-in-cryptocurrencies
- Aarjan Dhakhwa,*Crypto Currency And Its Effect In Nepal*,SPOTLIGHT NEPAL(Jun 16,2022,6 P.M.), https://www.spotlightnepal.com/2022/05/09/crypto-currency-and-its-effect-nepal/
- World Bank,*Personal remittances,received(% of GDP)- Nepal*,WORLD BANK GROUP(Aug 5,2022,8 P.M.), https://data.worldbank.org/indicator/BX.TRF.PWKR.DT.GD.ZS?locations=NP
- RatoJob, *Foreign Exchange Regulation Act 2019 | विदेशी विनिमय नियमन ऐन २०१९*, RATOJOB, https://www.ratojob.com/foreign-exchange-regulation-act/#:~:text=Objectives%20of%20Foreign%20Exchange%20Regulation%20Act%202019&text=To%20promote%20the%20use%20of,(BoP)%20in%20the%20nation , *archived at* https://perma.cc/PWG8-S9B8
- Nepal Rastra Bank, *Nepal Rastra Bank Act, 2058 (2002)*, https://www.nrb.org.np/contents/uploads/2019/12/Nepal-Rastra-Bank-Act-2002-English2074.12.21.pdf
- Nepal Law Commission, *Act Restricting Investment Abroad, 2021(1964)*, https://lawcommission.gov.np/en/wp-content/uploads/2018/10/act-restricting-investment-abroad-20211964.pdf
- Freeman Law's Article, *Nepal and Cryptocurrency*, https://freemanlaw.com/cryptocurrency/nepal/
- Techpana, *Why is Cryptocurrency banned in Nepal?*, https://www.youtube.com/watch?v=zdFyZMJDwjE
- Nepal Rastra Bank, *Bitcoin Notice*, https://nrb.org.np/fxm/notices/BitcoinNotice.pdf ,*archived at* https://perma.cc/856B-8JQ8

- Vildana Hajric, *Crypto Crash Erases More Than $1 Trillion in Market Value,* BLOOMBERG(Jan 21,2022), Crypto Crash Erases $1 Trillion in Value; Bitcoin (BTC), Ether (ETH) Prices Drop – Bloomberg
- *Why Can There Only Be 21 Million Bitcoins?,* ORIGINSTAMP, Why Can There Only Be 21 Million Bitcoins? | OriginStamp
- CFI Team, *Minting Crypto,* CFI (January 19, 2022), Minting Crypto - Overview, Process, Benefits (corporatefinanceinstitute.com)
- Brian Nibley, *What Does Burning Crypto Mean?,* SOFI(August 10,2022), What Does Burning Crypto Mean? How & Why Is It Burned? | SoFi
- Lubomir Tassev, *Nepal Prepares to Issue Digital Currency, Drafts Necessary Amendments,* BITCOIN.COM (August 7,2022), Nepal Prepares to Issue Digital Currency, Drafts Necessary Amendments – Finance Bitcoin News
- *Nepal nationals used crypto to divert fraud money to China*, THE TIMES OF INDIA (December 25,2021), Nepal nationals used crypto to divert fraud money to China | Hyderabad News - Times of India (indiatimes.com)