Outline:

Use selected on-line articles to explore current issues related to crypto currencies such as BitCoin. A focus for learning is: the underlying technologies, impacts on society, and impacts on the environment.

Objectives:

* C1.4 describe how electronic access to information influences our everyday lives.
* C2.1 describe the negative effects of computers and computer use on the environment.
* C3.1 describe legal and ethical issues related to the use of computers.

**Level 1: Cryptocurrencies & Blockchains**

Read the following resources before answering the questions below:

* <https://www.investopedia.com/tech/most-important-cryptocurrencies-other-than-bitcoin/>
* <https://www.investopedia.com/terms/b/blockchain.asp>
* <https://www.cryptoandgamers.com/>

1. **What is a “cryptocurrency” and how are “cryptocurrencies” different from traditional currencies (money)?**

“A **cryptocurrency** (or crypto currency) is a digital asset designed to work as a medium of exchange that uses strong cryptography to secure financial transactions, control the creation of additional units, and verify the transfer of assets.” - Wikipedia

“The “crypto” in cryptocurrencies refers to complicated cryptography which allows for a particular digital token to be generated, stored, and transacted securely and, typically, anonymously. “ - Prableen Bajpai

The main difference between cryptocurrencies and fiat money is that cryptocurrencies aren’t controlled by a bank, instead they are in limited databases named “blockchains” that nobody can change or manipulate in normal conditions.

Furthermore, cryptocurrencies are typically developed by coding teams who build in methods of supplying or distributing, also known as “mining”. Another main feature of cryptocurrencies is that they are free from government control.

1. **BitCoin is the leading cryptocurrency that most people know. What are some other cryptocurrencies and what are their unique features?**

* **Litecoin (LTC) :** Launched in 2011. It was among the first cryptocurrencies along Bitcoin. Founded by Charlie Lee. Litecoin is an open source global payment network which is controlled by any central authority and uses something called a "scrypt" as a proof of work. This can be decoded with the help of CPUs of consumer grade. Litecoin has a faster block generation rate and a faster transaction confirmation. *As of February 9, 2019, Litecoin had a market cap of $2.63 billion and a per token value of $43.41.*

### Ethereum (ETH) :Launched in 2015. Ethereum is a decentralized software platform. The applications on ethereum are run on a specific platform cryptographic token known as ether. Ether can be visualized as a method of moving across the ethereum platform, and are utilized most by developers looking to develop and run applications inside Ethereum. They are also used by Investors looking to make purchases of other digital currencies using ether. In 2014, ethereum had launched a pre-sale for ether which was met which a great response from its user base, this in turn helped to usher in the age of the initial coin offering (ICO). It can be used to “codify, decentralize, secure and trade just about anything.” In 2016, Ethereum split into Ethereum (ETH) and Ethereum Classic (ETC). *As of February 9, 2019, Ethereum (ETH) had a market cap of $12.49 billion and a per token value of $118.71.*

### Zcash (ZEC) : Launched in 2016. Zcash is a decentralized and open-source cryptocurrency. Zcash offers privacy and selective transparency of transactions, extra security or privacy. All transactions are recorded and published on a blockchain, yet additional details such as the sender, recipient, and amount remain private. Zcash also offers its users the option of “shielded” transactions, which permit for content to be encrypted using advanced cryptographic technique or zero-knowledge proof construction called a zk-SNARK (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge) developed by its team. *As of February 9, 2019, Zcash had a market cap of $291.25 million and a value per token of $49.84.*

““Zero-knowledge” proofs allow one party (the prover) to prove to another (the verifier) that a statement is true, without revealing any information beyond the validity of the statement itself. For example, given the hash of a random number, the prover could convince the verifier that there indeed exists a number with this hash value, without revealing what it is.” - ZCash

### Dash (DASH) : Launched in January 2014. Dash grants more anonymity as it operates within a decentralized mastercode network that makes transactions almost untraceable. Dash was created and developed by Evan Duffield. It be mined using a CPU or GPU. It has technological features known as DarkSend and InstantX. *As of February 9, 2019, Dash had a market cap of $640.76 million and a per token value of $74.32.*

### Ripple (XRP) : Launched in 2012. Ripple has real-time global settlement networks that offers instantaneous, certain and low-cost international payments. Ripple “enables banks to settle cross-border payments in real time, with end-to-end transparency, and at lower costs.” Ripple sets itself apart from bitcoin and many other altcoins by it’s consensus ledger (its method of conformation). That is unique in that it doesn’t require mining since Ripple doesn't require mining, thus it reduces the usage of computing power, and minimizes network latency. Ripple is one of the most intriguing digital currencies among traditional financial institutions looking for ways to revolutionize cross-border payments. *As of February 9, 2019, Ripple had a market cap of $12.69 billion and a per token value of $0.308.*

### Monero (XMR) : Launched in April 2014. Monero is a secure, private and untraceable currency.I t has a special technique called “ring signatures.”, this shows a group of cryptographic signatures which have at the very least one real participant. But since they all seem to be valid, the real one can’t be isolated. *As of February 9, 2019, Monero had a market cap of $808.50 million and a per token value of $48.18.*

### Bitcoin Cash (BCH) : Launched in 2017. Bitcoin Cash is one of the earliest and most successful hard forks of the original bitcoin. A fork takes place as the result of discussion amongst developers and miners. The decentralized nature of digital currencies incites wholesale changes to the code underlying the token or coin at hand to be made at general consensus. This process may varies according to the particular cryptocurrency. When groups can’t come to an agreement, sometimes the digital currency is split, with the original remaining true to its original code and the other copy becoming a new version of the prior coin, along with complete with changes to its code. Bitcoin Cash was a result of one of these splits. Bitcoin has a strict limit on the size of blocks which are 1 megabyte. It increases the block size from 1 MB to 8 MB, with the idea being that larger blocks will create faster transaction times. *As of February 9, 2019, BCH had a market cap of $2.23 billion and a value per token of $126.49.*

### 8) NEO (NEO) : Launched in 2014. It is the largest cryptocurrency from China and is sometimes referred to a “Chinese Ethereum” due to it’s similar use of smart contracts.

### 

### “Smart contracts can:

### Function as ‘multi-signature’ accounts, so that funds are spent only when a required percentage of people agree

### Manage agreements between users, say, if one buys insurance from the other

### Provide utility to other contracts (similar to how a software library works)

### Store information about an application, such as domain registration information or membership records.“ - Coindesk

### NEO’s success can be attributed to its support of programming in several languages, such as Go, Java, C++, and others. *As of February 9, 2019, NEO had a market cap of $492.48 million and a value per token of $7.58.*

### Cardano (ADA) : Launched in September of 2017. Cardano offers all of the perks of Ethereum, as well as many others. Cardo also claims to solve some of the most pressing problems affecting cryptocurrencies everywhere such as interoperability, scalability, international payments, etc. Due to its focus on this area, ADA was able to take an international payment processing times down from days down to seconds. *As of February 9, 2019, Cardano had a market cap of $1.16 billion and a per token value of $0.041.*

### EOS (EOS) : Launched in June 2018. Created by cryptocurrency pioneer Dan Larimer. EOS is designed after ethereum, thus it offers a platform on which developers can create decentralized applications. It had a high initial coin offering which was one of the longest and most profitable in history, pulling in around $4 billion funds through crowdsourcing efforts. EOS contains EOS.IO, similar to the OS of a computer and being the blockchain network for it and EOS coins. EOS also doesn’t have a mining mechanism to create coins.

1. “**Blockchains” are the basic technology behind cryptocurrencies and other emerging technologies. Explain blockchains work with respect to:**
   1. **What they store**

* Blocks store information about transactions.
* Blocks store information about who is participating in transactions.
* Blocks store information that distinguishes them from other blocks.
  1. **How they work**

A Blockchain is a type of diary or spreadsheet which contains information about transactions. Every transaction generates a hash which is a string of numbers and letters.Transactions are submitted in the order in which they occurred and the order of it is very important. A hash depends on the transaction and the previous transactions hash. A small change within a transaction creates a completely new hash. The nodes check to see if a transaction has not been changed by inspecting the hash.

“A node is a device on a blockchain network, that is in essence the foundation of the technology, allowing it to function and survive. ... Nodes are often arranged in the structure of trees, known as binary trees. Each cryptocurrency has its own nodes, maintaining the transaction records of that particular token.” - Lisk

If a transaction becomes approved by a majority of the nodes then it is written into a block. Each block refers to the previous block and together make a Blockchain. A Blockchain is very effective as it spreads over several computers, each of which have a copy of the Blockchain.

* 1. **How they are secure and private**
  + New blocks are always stored linearly and chronologically.
  + After a block has been added to the end of the blockchain, it is very difficult to go back and alter the contents of the block.
  + Each block contains a hash, along with the hash of the block before it. Hash codes are manufactured by a math function that turns digital information into a string of numbers and letters. If the information is edited in any way, the hash code changes as well.
  + If a hacker attempted to edit a transaction , as soon as they would edit the amount of the transaction, the block’s hash will change. The next block within the chain would still contain the old hash, so the hacker would need to update that block in order to cover their tracks. Although, doing so would change that block’s hash. And the next, and so on. Recalculating all those hashes would take an nigh impossible amount of computing power. Once a block is added to the blockchain it becomes very difficult to edit and impossible to delete.
  + To confront the issue of trust, blockchain networks have implemented tests knows as “consensus models.” They require users to “prove” themselves before they can be in a blockchain network. One of the most common examples employed by Bitcoin is called “proof of work.” In this system, computers have to “prove” that they have done “work” by solving a complex computational math problem. If a computer solves one of these problems, they are eligible to add a block within the blockchain. The process of adding blocks to aka “mining,” is not easy. According to the blockchain news site BlockExplorer, the probability of solving one of these problems on the Bitcoin network were about 1 in 5.8 trillion in February 2019. To solve complex math problems at those odds, computers must run programs at high amounts of power and energy.
  1. **How they use public and private encryption keys**

In the Bitcoin network, the blockchain is shared, maintained by a public network of users and agreed upon. After users join the network, their connected computer receives a copy of the blockchain that is updated whenever a new block of transactions is added.

1. **How does BitCoin use blockchains?**

Blockchain forms the bedrock for cryptocurrencies such as Bitcoin. Currencies like the Canadian dollar are regulated and verified by the banks/government. Under a central authority system, a user’s data and currency are at the control of their bank or government which means in a scenario where if a user’s bank collapses or they live in a country with an unstable government, the value of their currency is at risk. A Blockchain allows Bitcoin and other cryptocurrencies to operate without a central authority. This reduces risks and eliminates several processing and transaction fees. It also provides those in countries with unstable currencies a more stable option with more opportunities.

1. **What are some other real-world applications of blockchains?**

Blockchain technology may be used to store data about property exchanges, stops in a supply chain, and even votes for a candidate. Professional services network Deloitte recently surveyed 1,000 companies about integrating blockchain into their business operations. Their survey found that..

* 34% already had a blockchain system in production today
* 41% expected to deploy a blockchain application within the next 12 months.
* 40% of the surveyed companies reported they would invest $5 million or more in blockchain in the coming year.

1. **What are some advantages and disadvantages of blockchains?**

### Accuracy

***Advantages***

### Cost : Blockchain eliminates the necessity for third-party verification and, along with it, their associated costs. Bitcoin doesn’t have a central authority and has virtually no transaction fees.

### Decentralization : Refer to Question 4.

### Efficiency : Blockchain is working 24/7. Transactions can be finished in around 10 minutes and are secure after a few hours.

### Privacy : Users cannot access identifying information about the users making those transactions. When a user makes public transactions, their public key, is noted on the blockchain, rather than their personal information.

### Security : Refer to Question 3c.

**Transparency:** Due to it’s open source build, users on the blockchain network can modify the code as they want so long as they have a majority of the network’s computational power backing them. This makes tampering with data difficult since with millions of computers on the blockchain network at all times for example, it is unlikely that anyone could make a change without being noticed.

***Disadvantages***

### 

### Cost : The technology is far from free that is used for this. The “proof of work” system consumes unthinkable amounts of computational power. According to a study from research company Elite Fixtures, the cost of mining a single bitcoin from $531 to $26,170.

### Inefficiency: Bitcoin’s “proof of work” system takes around 10 minutes to add a new block to the blockchain. At that rate, it can be estimated that the blockchain network can only manage seven transactions per second and although other cryptocurrencies like Ethereum and Bitcoin Cash perform better than bitcoin, they are still limited by blockchain.

### Privacy : Illegal trading and activity can be done on the blockchain network. Refer to; Silk Road, an online illegal “dark web” marketplace operating from February 2011 to October 2013 before it was shut down by the FBI. Due to the immense privacy of cryptocurrencies, this can be considered a double edged sword as it grants illegal activities large amounts on anonymity.

### Susceptibility : Newer cryptocurrencies and blockchain networks are susceptible to 51% attacks.

“1% attack refers to an attack on a blockchain – usually bitcoin's, for which such an attack is still hypothetical – by a group of miners controlling more than 50% of the network's mining hashrate, or computing power. The attackers would be able to prevent new transactions from gaining confirmations, allowing them to halt payments between some or all users. They would also be able to reverse transactions that were completed while they were in control of the network, meaning they could double-spend coins.” - Investopedia

1. **Blockchain based games are the latest development in the gaming industry. Research the topic “Crypto Games” (google) to answer the following questions.**
   1. **What are some interesting Crypto Games available for Android or iPhone?**

**Sweatcoin:** grants “sweatcoins” simply for walking, “sweatcoins” will eventually be turned into actual cryptocurrency on a blockchain.

**Stormplay:** Do either low reward tasks or high reward tasks known as “bolts” .

**Alien Run:** You play as an alien avoiding obstacles thrown at you in return for Bitcoin. You can also level up your alien to claim rewards.

**Blockchain Game:** Align blocks with the last placed block, every 10 blocks you have the option to try claiming rewards or play more for a chance to receive more rewards.

* 1. **How are they different from conventional games?**

“Crypto games are, usually, browser based games that incorporate the use of smart contracts and a blockchain for some (or all) of the game’s features...The advantages of crypto games over regular games are very clear. The players actually own their purchased game assets, and even if the game dies or shuts down, they still have their asset in their wallet, and they can use it on neutral markets or integrate 3rd parties to use them.” - Exoplanets

**Works Cited**

Bajpai, Prableen. “What Are the 10 Most Important Cryptocurrencies Other Than Bitcoin?” *Investopedia*, Investopedia, 9 Feb. 2019, www.investopedia.com/tech/most-important-cryptocurrencies-other-than-bitcoin/.

ExoPlanets. “Crypto Games - A Niche? A New Genre of Gaming? Both.” *Medium.com*, Medium, 11 June 2018, medium.com/@exoplanets2018/crypto-games-a-niche-a-new-genre-of-gaming-both-eacf9c1fad4e.

Fortney, Luke. “Blockchain, Explained.” *Investopedia*, Investopedia, 10 Feb. 2019, www.investopedia.com/terms/b/blockchain.asp.

Frankenfield, Jake. “51% Attack.” *Investopedia*, Investopedia, 7 Feb. 2019, www.investopedia.com/terms/1/51-attack.asp.

“How Blockchain Technology Works. Guide for Beginners.” *Cointelegraph*, Cointelegraph, cointelegraph.com/bitcoin-for-beginners/how-blockchain-technology-works-guide-for-beginners#hash-function.

“How Do Ethereum Smart Contracts Work?” *CoinDesk*, CoinDesk, www.coindesk.com/information/ethereum-smart-contracts-work.

Lecky, Alex Masters, et al. “Top 5 Best Blockchain Mobile Apps That Help You Earn Cryptocurrency - Income for Savvy IPhone and Android Users.” *CRYPTONICLES*, 18 Dec. 2018, www.cryptonicles.com/posts/top-5-best-blockchain-mobile-apps-that-help-you-earn-cryptocurrency-income-for-s-22578880.

“What Are Zk-SNARKs?” *Zcash - How Zk-SNARKs Work in Zcash*, z.cash/technology/zksnarks/.

“What Is a Node? » Learn about Blockchain Tech | Lisk Academy.” *Lisk*, lisk.io/academy/blockchain-basics/how-does-blockchain-work/nodes.

**Level 2: Bitcoin & Society**

Read the following resources before answering the questions below:

<https://www.cnet.com/how-to/what-is-bitcoin/>

<https://www.independent.co.uk/life-style/gadgets-and-tech/news/bitcoin-price-fall-criminals-blockchain-anonymous-cryptocurrency-zcash-monero-dash-a8174716.html>

<https://coincenter.org/link/why-ransomware-criminals-use-bitcoin-and-why-that-could-be-their-undoing>

**1. Who created BitCoin and who owns BitCoin now?**

It was created by Satoshi Nakamoto in 2009. In 2011 Satoshi turned over the source code to others in the Bitcoin Community.

**2. How is BitCoin created and what is "BitCoin Mining"?**

A person can mine Bitcoin by doing complex math and record keeping. When someone sends a Bitcoin the network records that transaction, and the others are made over time in something known as a “block”. Computers running these “mining” softwares write these transactions in a Blockchain.

**3. Can you buy BitCoin and what does it cost?**

Using Coinbase you can deposit your national currency in exchange of digital currency.

**4. Why would you want to buy BitCoin and what can you use it for?**

* Selling It
* Holding On to It
* Buying NBA Tickets (Dallas Mavericks Only)
* Buy Burger King Whoppers
* Guns (America Only)
* Rolex Watches
* etc

**5. What are the risks of using BitCoin?**

Refer to Level 1, Question 6, *Disadvantages.*

**6. How much of BitCoin business is related to criminal activity?**

The University of Technology Sydney found that…

* 44% of Bitcoin transactions were associated with illegal activity
* 25% of all Bitcoin users were associated with illegal activity

They found in April 2017 that near 24 million Bitcoin market participants use Bitcoin primarily for illegal purposes.

**7. What are some of the reasons why criminals use BitCoin?**

### 

### Since it is electronic money it is simple to easy to create software to demand a payment along with simultaneously demanding that a payment has been made.

* Bitcoin is efficient due to it being fast, reliable, and verifiable. All a hacker has to do is just watch the public blockchain to check if and what time a victim has paid the money.
* A hacker can also make a distinct payment address for every victim. They can also automate the process of unlocking their files in a confirmed bitcoin transaction to that distinct address.
* Criminals also use BitCoin simply because its reliable and simply works

**8. What are some of the disadvantages of BitCoin when used for criminal activity?**

* The open source build of bitcoin blockchain transactions allows for the global community to watch the ransom money.
* In America, all the major bitcoin exchanges are regulated by FINCEN.
* Any money extorted from victims can be viewed on the bitcoin network, the exchange from bitcoin to fiat money is where criminals are vulnerable to being identified."
* A user’s bitcoin address is a number that stays with the user. By connecting that address to a single user, you can also identify and trace all of the transactions in which that account has done using that address.
* Law enforcement can use the bitcoin blockchain to track criminals

9.  **Many people dislike BitCoin because they think it is only good for criminal activity.**

**Is this true? Write a supported opinion paragraph (SOP) to explain your position.**

BitCoin is not something that is only good for criminal activity since it is valuable to have in possession, decentralized and is secure. These 3 reasons are enough to incite anyone to have Bitcoin. Bitcoin is valuable to have in possession.As of now 1 BitCoin is worth 5,180 CAD. To have around 5k CAD with only a single digital currency will be intriguing enough for anybody looking to make a profit.Bitcoin is decentralized. Due to BitCoins decentralized nature, you don’t have to worry about any Banks or Government making any major changes to it. Bitcoin is secure.With the use of a Blockchain, you can rest assured your BitCoin won’t be compromised anytime.Bitcoin is valuable, decentralized and secure. Although it’s value may fluctuate over time, you can never go wrong with having some Bitcoin.

**Level 3: Bitcoin & The Environment**

Read the following resources before answering the questions below:

· <https://www.cbc.ca/news/business/bitcoin-electricity-1.4668768>

· <https://www.cbc.ca/news/business/hut8-medicine-hat-bitcoin-mining-1.4834027>

**1. What is a BitCoin “miner” and why are people concerned about BitCoin mining?**

“a "mining rig" is a colloquial metaphor for a single **computer** system that performs the necessary computations for "mining".” - BitCoin Wiki

People are concerned about BitCoin mining due to the immense power it consumes, a BitCoin mining facility in Toronto consumed over 62 megawatts

BitCoin miners are also said to use 2.5 gigawatts of power.

**2. Why does BitCoin mining use so much energy?**

Bitcoin Miner solve puzzles with very specific requirements. A miner’s solutions and transactions are added to the blockchain. To make sure that coins will not be produced quickly, as the network’s computational power increases, the bitcoin procedure makes it harder to find a specific solution. Around every 2 weeks, the system is calibrated, thus miners are obligated to keep upgrading to earn BitCoin as fast as competitors. Along with upgraded computer power comes higher computer energy usage.

**3. Why has Hut-8 decided to locate its facility in Alberta when its head office is in Toronto? What does the city of Medicine Hat provide that is required for mining BitCoin?**

“"They could have gone anywhere in the world and they chose Medicine Hat," said Clugston. "[Hut 8] is not here for renewable energy because it is not reliable. They need gas-fired generation and we have it in spades."” - CBC News

Hut 8 decided to locate it’s facility in Alberta due to the high amount of power it produces from natural gas and electricity production.

**4. What benefits does the city of Medicine Hat expect to see from this BitCoin facility?**

Ted Clugston, the city’s mayor, claims that Medicine Hat will see financial boosts from the economic benefits provided by Hut 8.

**5. What concern does the city of Medicine Hat have about from this Bitcoin facility?**

The main issue with this Bitcoin Facility is that it consumes colossal amounts of fossil fuel energy and the increasing amounts of electricity it will consume.

**6.What concern do environmentalists have about the Medicine Hat facility and about BitCoin mining in general? E.g. how does BitCoin mining harm the environment.**

* Large Fossil Fuel Consumption
* Large Electricity Consumption
* Large Amounts of Carbon Emissions

**7.If Hut-8 wanted to build a facility in Brampton, would you be in favor of this proposal. Write a SOP to justify your position.**

**Introduction:** Building a facility in Brampton would could bring economic benefits but overall the cons outweigh the pros.Massive electrical usage will be required.As demonstrated in Hut 8’s facility in Alberta, it had consumed over 62 megawatts.  As time progresses the electrical usage will only increase to higher values straining our resources even more.Around every 2 weeks Bitcoin systems are recalibrated, forcing miners to upgrading to earn BitCoin just at fast as competitors. Along with upgraded computer power comes higher computer energy usage.BitCoins value is fluctuating so putting so much money into a facility with an unsure payback may not be the best idea. For context in Dec 15, 2017, a single Bitcoin had a worth of 25,271, now it’s only 5,399. All in all Building a facility would have perks but there are just too many downsides.

**Works Cited**

“Mining.” *B-Money - Bitcoin Wiki*, en.bitcoin.it/wiki/Mining.

“Why Bitcoin Uses so Much Energy.” *The Economist*, The Economist Newspaper, 9 July 2018, www.economist.com/the-economist-explains/2018/07/09/why-bitcoin-uses-so-much-energy.