THE FUTURE OF CRYPTOCURRENCY: EVALUATING ITS VIABILITY AS A SUSTAINABLE TECHNOLOGY AND ITS POTENTIAL IMPLICATIONS ON SOCIETY

by

ELLIOT TERNER

A THESIS

Presented to the Department of Computer and Information Science
and the Robert D. Clark Honors College
in partial fulfillment of the requirements for the degree of
Bachelor of Science

May 2023

An Abstract of the Thesis of

Elliot Terner for the degree of Bachelor of Science
in the Department of Computer and Information Science to be taken May 2023

Title: The Future of Cryptocurrency: Evaluating Its Viability as a Sustainable Technology and Its Potential Implications on Society

Approved: *Professor Joe Li, Ph.D.*
Primary Thesis Advisor

Cryptocurrencies are an extremely new and constantly changing technology that has been gaining tremendous amounts of popularity in the last several years. The underlying technology behind cryptocurrencies, blockchain, acts as a decentralized and distributed ledger for which it holds transaction information associated with the users of the network. This is beneficial to those who use these currencies because it allows for the network to be decentralized, transparent, and immutable. While for many, these benefits are very compelling, some argue that cryptocurrencies are simply a fad and do not possess a strong enough foundation to last into the future as our society changes. The aim of this thesis is to take this question head on, and assess the long-term viability of cryptocurrency, based on the underlying technology, the direction the industry is heading, public opinion, and many other factors. Additionally, this paper will explore the potential implications that would occur in our society as a result of a more widespread adoption of cryptocurrency. Based on all these factors, one outcome is certain for cryptocurrency; the future is unclear. Cryptocurrency is an extremely innovative and important technology with many undeniable benefits that come along with the technology, such as security, transparency, lack of centralized authority, and many more.

However, it is simply too new of a technology with many uncertainties to be able to determine with absolute certainty whether it will last into the future or not, as the answer to this question is extremely nuanced with many factors that make it impossible to determine a straightforward answer.

Table of Contents

Chapter 1: Introduction: 6

Purpose of Study: 7

Research Questions and Methodology 7

Literature Review: 9

Chapter 2: Blockchain Technology 11

Introduction 11

Merkle Trees 11

Blockchain Network 12

Consensus Algorithms 15

Proof of Work: 16

Proof of Stake 17

Types of Blockchain Networks 18

Smart Contracts 20

Chapter 3: Cryptocurrencies 22

Overview 22

Cryptocurrency and Blockchain 23

Types of Cryptocurrencies: 24

Cryptocurrency Technologies 24

Risks Associated With Cryptocurrency 27

Energy Consumption and Environmental Concerns 28
Government Involvement 30
Cryptocurrency Crimes 31
Chapter 4: Cryptocurrency Long-Term Viability 34
Overview 34
Current State of Cryptocurrency: 34
Market Evaluation 35
Public Opinion 36
Direction Cryptocurrencies Are Heading 38
Regulation and Oversight 38
Innovation in Cryptocurrency 39
Risk and Reward - Will It Last? 40
Implications of A Widespread Adoption 40
The Challenge of Regulating Decentralized Cryptocurrencies 43
Challenges as an Alternative Currency 44
Assessing The Risks of Cryptocurrency 45
Conclusion 47
Bibliography: 48

Chapter 1: Introduction:

Blockchain and cryptocurrency are two extremely new technologies. The first blockchain-based cryptocurrency, Bitcoin, was created in 2009 by Satoshi Nakamoto to provide an alternative payment system that did not rely on the need for a central bank or other institutions. The goal of Bitcoin was to provide ordinary people with more control over the financial system they were a part of, thereby shifting financial control away from banks and other institutions (Frankenfield, 2022). From its inception in the late 2000s, Bitcoin has led the way for many innovations in digital currency and has spurred the creation of countless other blockchain-based currencies, each of which offers solutions to different problems. Moving forward to 2022, there are more than ten thousand cryptocurrencies in circulation, many of which have a market capitalization of over $1 billion.

Cryptocurrencies, at face value, seem to have grown tremendously in the past decade, and, by many metrics, they have. Upon its release, Bitcoin had a value of around US$0.0008 - it was essentially a worthless currency for many years after its release, as many people did not understand it and could not see any inherent value in using it. Bitcoin was the first of this type of currency, and many people thought it was nothing more than a passing trend. Bitcoin at the time of writing this paper, now has a value of US$16,680, which is over a billion times what it was originally worth, and this type of growth has not only been seen in Bitcoin. Cryptocurrencies across the board have soared in recent years, leaving many feeling optimistic about the future of blockchain-based currencies. However, despite the numerous potential benefits cryptocurrencies offer, there are still many factors holding people back from a more mainstream adoption of cryptocurrency. These factors include difficulty understanding how cryptocurrencies function, cryptocurrencies being a relatively new technology, being inherently volatile, as well as concern

for the amount of energy these technologies produce and the effects that it has on our environment.

Purpose of Study:

Exploding in the past decade, blockchain has grown to be a wildly popular subject in tech communities. Many describe it as a "solution looking for a problem" (Ramaswamy, 2023), and, even in 2023, blockchain is still trying to prove its utility. The most popular application of blockchain is seen in its use in cryptocurrencies such as Bitcoin, and, while cryptocurrencies have grown tremendously since their inception, people are not sure if this is a technology that will amount to anything more than a fad. Because of this, many people are wary of a more widespread adoption of cryptocurrencies and are unsure if cryptocurrencies as a whole have a strong enough foundation to last into the future as a society. This is a problem for cryptocurrencies because they were inherently created as an alternative form of payment. The purpose of this study is to explore the potential implications of a more mainstream adoption of cryptocurrency and evaluate whether, from the existing literature in this field, blockchain-based cryptocurrencies have a strong enough foundation to last into the future as our society changes and progresses.

Research Questions and Methodology

The overarching goal of this study is to execute and perform an archival review of existing technical literature to understand the inner workings of blockchain, and more specifically how blockchain functions as an application for various cryptocurrencies. I aim to understand if cryptocurrencies have the potential to become more integrated into our society, or if it is something that will not withstand the test of time as our society progresses and changes. I

will be evaluating many technical papers as well as online articles covering the concepts of blockchain and its applications to currency transfer. I will be closely reading and analyzing these documents to draw any patterns and conclusions that I see between them. These patterns and conclusions I observe will give me insight into both the benefits and drawbacks that blockchain-based cryptocurrencies inherently have, thereby helping me to determine if cryptocurrencies provide enough value in our society to last. My research will be entirely qualitative, as a research paper of this nature does not inherently lend itself to a deductive design. Rather, an inductive study of pre-existing literature fits the goals of this paper much better. The conclusions that I draw from my research will lead to potential explanations for the questions I am pursuing, thereby offering a plethora of dense qualitative information. Before my formal research, I had an intermediate level of understanding of blockchain and how it functioned as a form of money transfer in a very general sense. I knew that blockchain was a very new technology that was gaining more and more traction every day. After my preliminary research, there seemed to be two questions that would always stand out to me:

- Is cryptocurrency simply a fad or is it a technology that has a strong enough foundation to last into the future as our society changes and progresses?
- Cryptocurrency has exploded in popularity in recent years. If this growth continued, what would the implications of a wider adoption of cryptocurrency in our society be?

I recognize that these types of questions will be, in many cases, extremely hard to answer, however, I aim to get as close as possible. Through my research, I plan to create a holistic review of how the various systems of blockchain function, and how this lends itself to currency exchange.

Literature Review:

When it comes to the literature regarding blockchain and its applications to money transfer, there are a plethora of sources around this topic that continue to grow quickly. These sources range from being purely technical to highly theoretical, with few offering a comprehensive enough background for someone not involved in the field to make and interpret their thoughts on the subject. One of the most common questions in the field of blockchain and its applications to money transfer is "Will this last?". There seems to be no doubt that blockchain is a technology that certainly will change the world in one way or another, but the general consensus of if cryptocurrencies will eventually become a mainstream form of currency is still up for debate for several reasons. Blockchain is a new idea for most people, they don't understand it at a level to be able to interpret their own opinions on the technology, and generally, they do not trust it, all of which have been holding back cryptocurrencies from becoming more widely adopted in our economy.

Although blockchain, and, more specifically, cryptocurrency, have become very popular in recent years, there are still many aspects of the technology that are holding it back from becoming more widespread and accepted. The way cryptocurrencies are created is through the process of "mining". Whenever someone tries to make a transaction using any form of cryptocurrency, that transaction must be verified by a piece of hardware. This hardware that verifies the transaction is a "mining" node that ensures that everything about the transaction is authentic and verified. Once the transaction is verified, a unit of the cryptocurrency is created. This whole process is very resource intensive and requires tremendous amounts of energy, which, as a result, leads to increased greenhouse gas emissions. This is one of the main concerns

for cryptocurrencies, as many argue that the tremendous amount of energy required to create these cryptocurrencies is not worth the effect that it has on the environment.

If there was one paper that influenced my research more than others it would undoubtedly be *Bitcoin: Future or Fad?* (Daniel Tut, 2022). This research paper discusses the reservations many people have regarding cryptocurrencies, such as their lack of physical value, and supports their findings with dense quantitative information. This scientific paper helped me understand the many barriers that blockchain has concerning cryptocurrency and ultimately it is what interested me in studying both of my research questions for this paper.

Cryptocurrencies have countless benefits that appeal to the general population. They are inherently decentralized, transactions can be made quicker, they are generally immutable, along with many other benefits. In our society today, it seems as though we are at the point in which we are unsure if the benefits outweigh the negatives and uncertainty that inherently come with cryptocurrency. My research aims to examine a variety of sources that cover both the positive and negative aspects of blockchain's applications to cryptocurrency and assess whether this is enough to ensure that cryptocurrency will last into the future as our society changes.

Chapter 2: Blockchain Technology

Introduction

Blockchain technology is a distributed and immutable ledger, which is essentially a way to store and keep track of information related to what the blockchain is being used for. This data is stored in the "blocks" of the blockchain, which are simply containers for which the data in the blockchain is stored (Hayes, 2022). Each one of these blocks makes up a section of the blockchain and, within each one of them, there are several identifying characteristics associated with them. Each "block" contains the data that is being recorded (for example, transaction information regarding cryptocurrency), a hash value associated with the current block, and the hash value of the previous block within the blockchain. A hash value is a unique value linked to each block within the blockchain which is used to distinguish one block from another. By having a hash value associated with each block, the blockchain can be indexed so that information within each block can be later accessed whenever it is needed. By also storing the previous hash value of each block, this allows the blocks to be linked together and therefore immutable. This is important regarding security, as the information stored within the blockchain is oftentimes sensitive.

Merkle Trees

As previously discussed, blockchain technology is a way of storing data and information in structures called "blocks", which are linked together using the hash values of previous blocks. However, what is not as clear is how each block stores the information contained within it. This is where Merkle Trees come into play. Named after computer scientist Ralph Merkle, a Merkle Tree is a data structure used in blockchain technology to summarize and verify the information

stored within each block (Frankenfield, 2023). A Merkle Tree is simply a binary tree that is structured in a way to hold the information stored on the given blockchain network it is a part of. This means that all the nodes within the tree point to, at most, two other nodes. In the case of Merkle Trees, all of the information being stored in the network is found at the bottom of the tree at the leaf nodes, where all of the non-leaf nodes represent the hash value of their children's nodes. At the very top of the tree, there is a root node, called the Merkle root, which represents all of the information stored within the block, as its hash value was created as a result of combining all of the hash values of its children within the tree.

The application of Merkle Trees within blockchain technology provides several benefits, one of the most significant being its ability to allow for extremely efficient validation of the information stored within the blockchain network. With a Merkle Tree, other nodes within the network who are validating the information of the current block do not need to download the entire Merkle Tree to verify one segment of data. Instead, the nodes that are validating the information in the tree simply need to download a copy of the path on which that data is stored. This allows for much more efficient retrieval of data as there are sometimes thousands of data segments stored within the tree, and downloading the entire tree would be very computationally expensive for the nodes reviewing the data, which would lead to slower processing times for verifying the data that the tree holds.

Blockchain Network

Blockchain is considered a distributed ledger because of the way it is structured. Blockchain technology is made up of nodes within a network that can communicate with each other to carry out certain processes regarding the blockchain. Each one of these nodes has a record of the blockchain, which is what allows the network to be distributed, as all the nodes

thereby share the same information. Each one of these nodes is a processing unit that carries out complex calculations necessary to update/validate the blockchain with new information as needed. This process is called “mining”, and the type of calculations that are carried out in this process depends on the type of consensus algorithm being used by the blockchain network.

Structuring blockchain technology in a distributed fashion is no accident. There are countless benefits of having a distributed ledger (such as blockchain) over a centralized network, and these benefits are even more pronounced when examining the type of data that is oftentimes stored within a blockchain network. It’s important to have a blockchain network be distributed as opposed to centralized to prioritize security, transparency, reliability, as well as trust with those who use the network.

The type of information stored within a blockchain is oftentimes very sensitive and important to the people who have added it to the network, and it is for this reason that it is so important to prioritize security in the way a blockchain network is structured. A distributed ledger allows for the information within the network to be stored on all nodes that make up the blockchain. This decentralization helps to ensure that no single point of failure within the blockchain could bring down the entire network, as each node needs to agree on the information contained within a block before being updated (SoFi, 2022). For example, if an adversary were to attempt to manipulate transaction data stored within the Bitcoin network block, this would be virtually impossible, as the rest of the nodes in the network would not agree on the changes being made to the block, and the changes would not be implemented to all other versions of the blockchain.

One of the foundational goals of blockchain is to be transparent to the people that use it, which is why it is so crucial for a blockchain network to be structured in a way that prioritizes

this feature. Having a distributed network of nodes that all share the same information, allows for any one of these nodes to verify any information within the blockchain network, while still being considered secure against potential adversaries. This makes the network very transparent as any single node can independently verify the information stored within the network.

The information stored within a blockchain network is oftentimes very sensitive, which means that reliability needs to be prioritized in the way the blockchain network is structured, to ensure the safety of the data that is being stored. Having a distributed network of nodes that make up the blockchain, means that if any node were to fail for one reason or another, the rest of the nodes that make up the network would still be able to function and maintain the integrity of the data being stored in the network.

Finally, one of the main reasons blockchain was created in the first place was to ensure trust in those that contribute to the network. Having a distributed network of nodes that make up the blockchain network removes the need for a centralized authority or intermediary to control the network. In a centralized system, the control lies with a single party or entity, which can lead to issues such as corruption, censorship, and unequal access to information. On the other hand, a distributed blockchain network is controlled by a network of users who collectively verify and maintain the integrity of the data stored on the blockchain. This decentralized structure ensures that no one party has complete control over the network and creates a system of checks and balances that promotes transparency and fairness. Additionally, the cryptographic algorithms used in blockchain technology provide a high level of security, which further increases trust amongst network participants. Because the network is transparent, secure, and decentralized, all parties can transact with each other with a high level of confidence, knowing that the information

they are interacting with is trustworthy and that their transactions will be recorded accurately and securely.

Consensus Algorithms

The way a blockchain network is structured inherently calls for some way to verify the state of the blockchain along with all the associated nodes, and this is where blockchain consensus algorithms contribute. A blockchain network is a distributed and immutable ledger, which means that there is no centralized authority to verify the state of any block within the blockchain, the data it holds, or the entire blockchain itself (Frankenfield, 2023). Take, for instance, a traditional banking system. The bank uses a centralized database that stores customer account information, transaction history, and other sensitive data. The bank acts as the central authority and has complete control over the database, which means that it is responsible for verifying the accuracy and security of the data. In a blockchain network, there is no single authority to verify the data being stored in the blockchain, and, to compensate for this, a blockchain consensus algorithm is used.

A blockchain consensus algorithm is a set of rules and protocols that determine how the individual nodes within the blockchain network can reach an agreement on the state of the blockchain and the data it stores. The driving idea behind these consensus algorithms is to ensure the integrity of the blockchain and to prevent any malicious activity or fraud from adversaries trying to access the data stored within the network. There are many different types of blockchain consensus algorithms that all work towards these fundamental goals, and there are a handful of ones that are most used: Proof of Work (PoW) and Proof of Stake (PoS).

Proof of Work:

Proof of work is a blockchain consensus algorithm used in many blockchain networks, such as Bitcoin and Ethereum. In this algorithm, the nodes within the network ("miners") compete to solve complex mathematical problems known as "hash puzzles" to validate newly requested additions to the blockchain, which, in the case of cryptocurrencies, involve transaction data. After completing the hash puzzle, these miners are rewarded with newly created cryptocurrency for providing their computational resources. The difficulty of the hash puzzle is adjusted regularly to ensure that the rate at which new blocks are added to the blockchain stays consistent. The hash puzzle itself consists of finding a number (nonce) that, when combined with the information contained within the current block, produces a hash value with a certain amount of zeros in front of the hashed value. Miners use hardware that is optimized for these types of computations, such as ASICS, to complete these problems as fast as possible, thereby leading to a higher rate of receiving the newly minted cryptocurrency.

Proof of work is considered to be a secure consensus algorithm as it requires a significant amount of computational resources to complete the algorithm. For an adversary to successfully execute an attack on a blockchain network that uses proof of work, they would need to have control of over 51% of the network's computing power, which, in reality, is almost impossible, especially with the amount that blockchain networks have grown in recent years. Despite its widespread use, PoW has also been criticized for its extremely high energy consumption as well as the potential for centralization of the mining/ computational power within the network - In some cases, a large portion of the network's computational power is contained within a handful of mining networks ("pools"). This is a potential issue for these networks as these mining pools

often allow people to rent their computational resources, meaning that, with enough money, only a small number of pools would be needed to take over a network.

Proof of Stake

Proof of Stake (PoS) is a blockchain consensus algorithm used to allow the nodes of a blockchain network to meet a consensus on the state of the blockchain - it is the process used to validate new information being added to the network to ensure its security. Most commonly, this consensus algorithm is used in cryptocurrencies as a way to validate new transaction information that is being added to the network, although there are certainly other applications for this consensus algorithm in other industries, such as supply chain management, health care, or any other industry in which a strong consensus is needed to add new information to the network. PoS has been gaining popularity as a potential alternative to the more common consensus algorithm, Proof of Work, as it offers many benefits that some view more favorably than PoW. Proof of Stake differs from Proof of Work in the way nodes within the network validate/agree on new information being added. Nodes within the network (also known as "validators" or "forgers") are chosen to create new blocks and validate transaction data, based on the amount of cryptocurrency they hold, or "stake" on the network - this is where the name, Proof of Stake, comes from.

The driving factor behind the security associated with this type of consensus algorithm is the stake that these validators hold in the network. When new transaction data is initiated to the network, all of the nodes within the network will receive a copy of it and are tasked with validating the transaction information, adding it to a new block, then broadcasting the new block to other nodes within the network to be validated, before finally being added to the network. Nodes that hold more cryptocurrency within the network are given a higher priority when

determining which validators to create the new blocks, because, as the name implies, these nodes are “staking” their cryptocurrency as an incentive to create legitimate blocks with legitimate transaction information. If a validator, for any reason, broadcasts a block that is considered invalid, the other validators within the network will flag the transaction block, terminate it, and the validator who originally proposed the block will lose a portion of their cryptocurrency or “stake” in the network. The stake that these validators have in the network is what allows PoS to function at all - with no incentive to validate legitimate information in the network, there would be no reason for an adversarial node to not manipulate transaction information that goes against the network's protocol.

Types of Blockchain Networks

In recent years, blockchain technology, along with its many applications, has become increasingly popular for its ability to store and share data transparently. One of the key features that distinguishes blockchain from other forms of data storage is its ability to provide a decentralized ledger that anyone can access with the appropriate permissions. Although sharing many of the same characteristics, there are two main types of blockchain networks, both of which have various trade-offs between them: permissioned and permissionless.

Permissioned blockchain networks are blockchain networks that require the user of the network to have some level of authority/ permission to access the network. In other words, the network is restricted to only those who meet the network’s protocol. This means that all of the nodes within the network will first need to meet these requirements before beginning to validate transactions, view transaction data, or do anything else involving accessing the data within the network (Sharma, 2022). Permissioned blockchain networks are often used in industries and organizations that require a high level of control over their information, such as the banking

industry. The main advantage of a permissioned blockchain network is that there is a significantly higher level of security and control over the data that the network holds, although this means there is inherently less transparency regarding how the data is viewed.

In contrast to permissioned blockchain networks, permissionless blockchains, as the name implies, are open to anyone who wants to participate within the network. In other words, no permission, authority, or central authority is required to access the network and the data that is stored within it. However, this does not mean that there is no validation process for adding new or verifying existing information within the network - this simply means that the people who carry out these operations are not chosen based on their level of authority/ permission within the network. All of the nodes and participants within the network have the same level of access to the network. Although this level of transparency and lack of mediation from a trusted party may seem excessive and counterproductive to the overall health of the network, there are many instances in which a permissionless blockchain network is far more advantageous than a permissioned network.

Permissionless blockchain networks are often used by decentralized systems that require a high level of transparency within the network, and one of the most common applications of this is seen in cryptocurrency. The fundamental belief and goal of these currencies are to provide its user with an alternative form of currency compared to traditional fiat currency, while taking out the need for any sort of "middle-man" in the process, such as a central bank or governing body. This is where permissionless blockchain networks fill in the gap - by allowing anyone to access the network and validate the information stored within it, this removes the need for any sort of third party to verify transaction information for each transaction or transfer made with these cryptocurrencies. The network, along with all of the nodes that have chosen to contribute to it, is

responsible for validating transaction information, thereby removing the need for a third party. Although very fitting for the fundamental needs of cryptocurrencies, this does not mean that permissionless networks are perfect for all scenarios. The main disadvantages of these types of networks are their lack of control over data as well as potential security risks - both of which stem from the fact that anyone can access the data stored in the network structure in this manner.

Smart Contracts

Smart contracts are a revolutionary innovation in the field of blockchain technology, as they provide a decentralized and automated way of executing certain agreed-upon actions between parties using the blockchain network. Essentially, a smart contract is a self-executing program that is stored on the blockchain network to carry out certain tasks that are needed by the network and the people using it (Khan, 2021). These programs are designed to allow for, verify, and enforce the performance of traditional contracts, as a means of removing any intermediaries or a central authority from overseeing this process. One of the main reasons blockchain was created in the first place was to allow for a decentralized, secure, and efficient transfer of data without the need for a centralized authority, which is exactly what smart contracts accomplish. By having a computer program that is designed to carry out certain actions automatically within a blockchain network, it removes the need for any third party to be involved within the network.

Smart contracts are written in programming languages that are specifically designed for smart contracts, with one of the most common being Solidity, which is the programming language used to write smart contracts for the Ethereum cryptocurrency. Smart contracts can be used for a wide range of applications including supply chain management, voting system integration, and, most commonly, assisting in financial transactions. For example, in the Ethereum blockchain, a smart contract could be written to mimic the functionality of Kickstarter

- a crowdfunding platform to help startups. The main functionality behind Kickstarter is that individual donors can contribute to a project they have an interest in, and, if the crowdfunding goal is reached, the money they donated will go towards the development of their project, otherwise, the money will be given back to the donors. With smart contracts, this same functionality can be achieved using Ethereum. A smart contract could be written in such a way to allow individual donors to donate their Ethereum to a specific address, and, if the desired amount is reached, the address will keep the Ethereum and use it for the development of the project, and, if it is not met, the Ethereum will be transferred back to the donors. This is just one of the many examples of how smart contracts can be used to execute certain actions based on set criteria.

Chapter 3: Cryptocurrencies

Overview

Cryptocurrencies have become a revolutionary advancement in the world of technology and finance. They are digital currencies that use blockchain technology to create an alternative form of payment for their users. What makes these cryptocurrencies so groundbreaking is the way they fundamentally function. Cryptocurrencies operate without a third party, such as a banking institution or central government. Instead, these currencies are run on a blockchain network that contains countless nodes, all of which have all of the information stored on the network. These nodes on the network are the ones responsible for validating transactions, adding new transactions to the network, and checking the work of other nodes. This means that there is no need for a third party or central authority to be responsible for facilitating transactions using these cryptocurrencies because the network automatically regulates itself. While their inherent lack of authority may seem like a positive attribute for cryptocurrencies, this is not the case for all individuals. Many governments, government officials, along with many others look down on cryptocurrencies for their lack of control and ability to hide large sums of money.

The first cryptocurrency that was developed was Bitcoin, which was launched in 2009 by Satoshi Nakamoto in response to the 2008 financial crisis, which highlighted the many flaws associated with traditional banking systems. Since the creation of Bitcoin, thousands of cryptocurrencies have been created, one of the more noteworthy being Ethereum, which was launched in 2015, with the hopes of integrating new technologies such as smart contracts and the creation of decentralized applications.

Over the past decade, the cryptocurrency market has grown tremendously, with a total market capitalization of all cryptocurrencies reaching over $1.2 Trillion as of April 2023. Bitcoin

remains the largest and most used cryptocurrency, making up over 40% of the total market capitalization of all cryptocurrencies, while Ethereum, the world's second-largest cryptocurrency makes up about 20%, at a market capitalization of about $240 billion. The rest of the cryptocurrencies in circulation individually fail to make up even 10% of the total market capitalization for cryptocurrencies.

While there have been select businesses and corporations who have started to accept cryptocurrencies as a form of payment, the vast majority of places still do not consider them as a legitimate way to make purchases. Despite this, cryptocurrencies have gained popularity in recent years as a form of investment, with many of its bearers not even attempting to use them as currency at all. Despite their numerous benefits in security, privacy, and transparency, cryptocurrencies are not without their challenges and criticisms.

Cryptocurrency and Blockchain

Cryptocurrencies and blockchain technology are intrinsically related, in that cryptocurrencies simply use blockchain technology as a means of storing and handling the transactions made with them. A blockchain is an immutable, distributed ledger, and cryptocurrencies simply use this structure as a means of holding the data associated with their cryptocurrency, which is primarily made up of transaction information, along with other vital information related to the current block such as the reference to the previous block and a timestamp of when the block was created (Jara, 2022). Once one of these blocks is completed and all of the necessary information is added and verified, the block will be uploaded to all of the nodes within the network to permanently be added to the network. Once published, it is virtually impossible to make changes to any of the blocks within the chain.

Blockchain technology is used for cryptocurrencies because it provides a safe and transparent way to record and validate transactions made with the cryptocurrency being used. Unlike traditional ledgers that rely on a central authority such as a bank or governing body, the infrastructure that blockchain provides to cryptocurrencies allows for no third party to be a part of the process when making transactions or validating them. Instead, the blockchain network that a cryptocurrency uses instead relies on a consensus among the nodes of the network to keep a cryptocurrency functioning, thereby eliminating any need for a third party to be involved in the process.

Types of Cryptocurrencies:

As of April 2023, there are thousands of cryptocurrencies in circulation, each with its unique features and characteristics. While all cryptocurrencies use blockchain technology as the structure for how they store their data and have some overlapping characteristics, they can also vary dramatically depending on the underlying technology used in the cryptocurrency, the purpose that the currency is intended for, as well as how governments are involved with them in the first place. All cryptocurrencies have certain attributes associated with them that make them better in certain situations than in others (Sofi, 2022), so it is important to consider what values and functionalities a cryptocurrency offers before determining which one best fits someone's individual needs.

Cryptocurrency Technologies

Although they share many of the same features, what makes cryptocurrencies fundamentally different from one another, in terms of how they function, is the technology that is used to develop them, such as the type of consensus algorithm used, block time, block size, and

many other miscellaneous attributes. All of these factors determine how efficient and secure a cryptocurrency is along with the underlying functionality of the currency as a whole. This means that, depending on what goals an individual has, different cryptocurrencies might be better suited than others.

One of the most obvious and important technologies that determine how a cryptocurrency functions is the type of consensus algorithm being used on the cryptocurrency network. A consensus algorithm is an underlying protocol that determines how a cryptocurrency verifies, validates, and adds transaction data to the cryptocurrency network, as there is no centralized authority to do this. Instead, the nodes that make up the network must contribute their computing power to run these algorithms to constantly verify the state of the blockchain.

One of the most commonly used consensus algorithms is Proof-of-Work (PoW), which is used by the most widely used cryptocurrency - Bitcoin. This model functions by using the computing power of all of the nodes within the network to verify transaction data as it is received by the network. This type of consensus algorithm is considered secure due to the extremely high amount of computational power required to verify transaction information, although this inherently leads to slower and less efficient transaction times. Additionally, many environmentalists have argued that the amount of energy that the nodes within the network use for this algorithm is leading to environmental concerns. This algorithm has many attributes that make it useful for cryptocurrencies, but there are still many drawbacks associated with its high energy consumption and processing times.

On the other side of the energy-consumption spectrum, a slightly less common consensus algorithm, Proof-of-Stake (PoS) leverages the cryptocurrency held by the users of the network as a means to ensure the validity of the transaction data in the network along with increasing overall

efficiency. Proof-of-Stake ensures the state of the blockchain by having its users "stake" the cryptocurrency they hold to ensure that the information they validate is correct (Sergeenkov, 2021). If one of the nodes within the network were to validate information on the network that was incorrect, they would lose a position of their stake, and the information would not be added to the blockchain. This "stake" that they have in the network is what incentivizes nodes to validate transaction information correctly. While this does lead to significantly faster transaction times, as there is no need for the nodes of the network to solve unnecessarily computationally expensive puzzles (as seen in PoW), at the same time, this means that there is an inherently more centralized authority within the network as some users can carry a significant portion of the network's total cryptocurrency in circulation. For a PoS consensus algorithm, this inherently leads to more control over the network, as users with more cryptocurrency to stake are given a higher priority to validate transaction information.

The block time is another factor that differentiates how cryptocurrencies function. Block time refers to the amount of time it takes for a new block containing transaction information to be added to the network. For example, Bitcoin has a block time of 10 minutes, Ethereum is around 12 seconds, and Litecoin is around 2.5 minutes. Apart from efficiency, block time also contributes to how securely information can be added to a cryptocurrency network. Cryptocurrencies with higher block times, such as Bitcoin, are generally considered to be more secure than ones with slower block times, as there is more time for the network to verify the legitimacy of the transaction information being proposed. On the other hand, in a cryptocurrency network like Ethereum, there is not nearly as much time to verify the transaction information and is therefore considered less secure in this regard.

Block size is another important factor to consider when quantifying the differences between various cryptocurrencies. In the case of cryptocurrencies, block size refers to the amount of transaction information each block within the blockchain can hold. For example, Bitcoin has a block size limit of 1MB per block, meaning that only a certain number of transactions can be held within the block before reaching the 1MB limit. Other cryptocurrencies, such as Bitcoin Cash offer block sizes of up to 32MB. Cryptocurrency networks that have smaller block sizes can sometimes lead to delays in transactions as well as higher transaction fees as there are periods where not all of the transactions can be processed instantly. Cryptocurrencies with larger block sizes fix this issue, as more transactions can be processed at the same time, but this inherently leads to more centralization, because fewer members of the network can afford the computational resources to support the block size of the network.

Risks Associated With Cryptocurrency

Cryptocurrencies have become a disruptive force in the world of finance and banking, offering a secure, decentralized, and transparent means of making transactions without the need for an intermediary, such as a traditional banking institution. However, while there are many benefits to these currencies over traditional fiat money, they have also generated many concerns involving energy consumption, environmental impacts, price volatility, and their role in criminal activity. These risks do not necessarily mean cryptocurrencies should be avoided altogether, but they should be factored into one's decision when considering whether or not to use a cryptocurrency.

Energy Consumption and Environmental Concerns

One of the most prominent criticisms of cryptocurrencies is the amount of energy they use to function, and the inherent environmental impacts that this leads to. The process of "mining" cryptocurrency involves the users of the network who contribute their computational resources to verify transaction information being added to the blockchain, as well as ensuring the state of the blockchain is legitimate. This process involves using the computational resources that the users provide to solve complex mathematical hash puzzles to validate newly requested additions to the blockchain. This uses a tremendous amount of energy as the number of calculations typically needed for miners to verify a block of transactions requires approximately 80,000 times more computational power than a traditional credit card transaction.

The majority of cryptocurrencies in circulation use the consensus algorithm, Proof-of-Work (PoW), which requires the nodes of a cryptocurrency network to solve these complex mathematical problems to verify the transaction information stored within the blockchain. As discussed previously, this whole process is extremely energy intensive and uses far more total energy than traditional banking systems, with estimates suggesting that the mining process involved in Bitcoin alone accounts for approximately 0.5% of global energy consumption (Carter, 2021). There are two trains of thought when it comes to interpreting how to view this staggering amount of energy consumption involved with cryptocurrencies. On one hand, those who support cryptocurrency use in our society believe as though this is a small price to pay for an alternative payment system, and, on the other hand, many believe as though this amount of energy consumption is unjustified given that there is no physical product produced by the Bitcoin network or any other cryptocurrencies for that matter.

Regardless of which train of thought one decides to believe in, the amount of energy consumed by these cryptocurrency networks has had significant environmental impacts. The massive amount of energy required to maintain cryptocurrency networks contributes to significantly higher greenhouse gas emissions than there would be otherwise, which will accelerate climate change over a long enough period. The amount of energy consumed by making a single Bitcoin transaction is roughly equal to over 700,000 Visa transactions and over 50,000 hours of watching YouTube (Field, 2021). Although hard to quantify exactly, in total, the amount of energy consumed across all cryptocurrency networks is roughly equivalent to the energy consumed by a mid-sized country. Not only this, but cryptocurrency mining technology is constantly advancing, leading to tremendous amounts of electronics waste, as older, less efficient miners become obsolete, and are replaced by newer models. As it stands, the amount of energy consumed by cryptocurrency networks has led many to question if the benefits they bring outweigh the significant environmental impacts that come along with the technology.

To address some of these environmental concerns, certain cryptocurrencies have used a newer consensus algorithm, Proof-of-Stake (PoS). This consensus algorithm functions fundamentally differently from Proof-of-Work in that it relies on the users of the network to stake the cryptocurrency they hold as collateral for ensuring that the transaction information they view, validate, and add to the blockchain network is legitimate. This is fundamentally different from PoW in that, to ensure the integrity of the network, this algorithm leverages the fact that contributors of the network will, more often than not, validate legitimate information, as they do not want to lose any of their staked currency. This contrasts with the PoW consensus algorithm which functions by completing complex mathematical problems which require tremendous amounts of energy. Without the need for these extremely resource-intensive algorithms, this type

of consensus algorithm uses far less energy and therefore has a much smaller carbon footprint when compared to other consensus algorithms.

Government Involvement

Governments around the world have taken many different approaches to regulating cryptocurrencies, each of which has differing levels of government involvement. Some governments, such as El Salvador, have integrated the currency into their economy by recognizing it as a legitimate means of payment, while other countries such as China have banned it altogether, even going so far as to imprison those who are involved with its activity. However, regardless of if a country supports the use of cryptocurrency or not, there is still one glaring issue that all governments must deal with when it comes to cryptocurrencies: decentralization.

One of the main challenges that governments must consider when trying to regulate cryptocurrencies is their decentralized nature. Fundamentally, all cryptocurrencies use blockchain technology as a way of creating a decentralized ledger for whatever information the network is trying to store. In the case of cryptocurrency, this means that there is no centralized authority that can control the transfer of funds between people on the network. Additionally, while governments can view the transactions being made with cryptocurrency, they are oftentimes still unable to determine who is involved with the transactions as the names of the people involved are not associated with each one of the transactions being made, instead, the transfer of funds is made between two addresses, often referred to as “wallets”. This makes regulating and taxing the transactions being made with cryptocurrencies close to impossible as it is exceedingly easy for users to hide their transactions or be dishonest about the amount that they report. This has led some governments, such as Switzerland, to take more of a hands-off

approach when it comes to cryptocurrencies, allowing them to exist outside of many regulatory frameworks

However, other governments, such as the United States, have taken a much more proactive approach to regulating cryptocurrency usage by implementing frameworks that specifically address the regulatory concerns that governments are faced with. The goal of these frameworks is to encourage the users of cryptocurrencies to be more transparent with the transactions they are making, thereby reducing the chances of any illicit activity involved with cryptocurrencies. While these frameworks certainly help to regulate the cryptocurrency market, there are still plenty of individuals who use cryptocurrency as a means for exercising illicit activity

Cryptocurrency Crimes

As cryptocurrencies continue to grow and expand into new markets, so does the amount of criminal activity associated with these currencies. Due to their decentralized nature, along with their relatively low governmental oversight, cryptocurrencies are exceptionally vulnerable to exploitation by adversaries wishing to use them as a tool to profit off of maliciously. Some of the most common forms of these cryptocurrency crimes include hacking and money laundering.

The most common form of cryptocurrency hacking involves gaining access to a user's accounts on a given cryptocurrency exchange. Hackers will use malware to gain access to a user's device, such as a laptop or mobile device, and, once the hacker has access to the device, they will be able to either access their digital wallet directly or go to the cryptocurrency exchange that they use and transfer the funds that they have to a different account of their choosing.

Another common form of cryptocurrency hacking involves phishing scams. In a phishing attack, the adversary will send some form of message to the target such as an email or text that will seem as though it is from a legitimate source, such as a cryptocurrency exchange. From there, the user will typically be prompted to input their login credentials, which is a normal request from cryptocurrency exchanges. In reality, the target is simply giving the hacker access to their login credentials, which will grant them access to the cryptocurrency stored in their wallet. From there, the attacker will transfer the currency from the target's wallet to another wallet of their choosing, which can happen in a matter of seconds in some cases. In response to these threats, cryptocurrency companies have begun using additional levels of security, such as two-factor authentication and encryption to protect the users' funds, which have proven to be relatively effective. However, while these added levels of security certainly do help to eliminate some of the malicious activity associated with cryptocurrencies, hackers continue to find new ways to attack these systems and exploit their vulnerabilities to gain access to users' funds, so it is extremely important to always be up to date with new security measures being implemented by these companies.

Perhaps the most common cryptocurrency-related crime, money laundering, has become a big problem for governmental bodies to deal with and regulate. Cryptocurrencies inherently offer significantly more anonymity when compared to traditional fiat currency as a result of their distributed structure, which criminals leverage as a way to launder their oftentimes illegally obtained cash. There are numerous ways criminals will initially turn their cash into cryptocurrency, but one of the more common ways is by using a Bitcoin ATM, which allows its users to deposit cash which it will convert into cryptocurrency. From there, the criminal will typically mix their cryptocurrency with other funds through a process known as "mixing", which

will obscure their transaction history even more. Regardless of which method criminals decide to use to launder their money, the result will be the same; their money will be converted into cryptocurrency and their transaction history will be almost impossible to follow, thereby leaving governmental bodies with very little to find the criminal.

Chapter 4: Cryptocurrency Long-Term Viability

Overview

In recent years, cryptocurrency has become a hot topic and major technological innovation, leading many to become involved with the technology either as an interest or investment. However, despite the many technological advancements that cryptocurrencies have over traditional fiat money, there are still many who are unsure if these benefits justify the use and development of cryptocurrencies in the first place, with many arguing that it is simply a fad. This chapter aims to address these concerns by providing a comprehensive analysis of the current state that cryptocurrency is in, examining alternative technologies to blockchain technology, weighing the benefits of cryptocurrencies with their inherent risks, and, finally, determining the direction that cryptocurrencies are headed in.

Current State of Cryptocurrency:

To assess the long-term viability of cryptocurrencies, we need to not only understand the underlying technologies behind them but also must understand the current state of the cryptocurrency market in recent history. Understanding how the cryptocurrency market is positioned in today's economy will help us gain insight into both its vulnerabilities, as well as the areas that it has excelled in. Furthermore, in the last several years, there have been many significant economic fluctuations and global events that have significantly affected the cryptocurrency market, and understanding how cryptocurrencies responded to these events will help us understand whether or not cryptocurrencies and the technologies behind them have fostered a strong enough foundation for cryptocurrencies to last into the future as our society progresses.

Market Evaluation

In the last 4 years, beginning with the start of the coronavirus pandemic, cryptocurrencies have seen drastic changes in their evaluations. The pandemic created several unique circumstances that initially led to a huge rise in the cryptocurrency market capitalization across the board, and by understanding how cryptocurrencies responded to these types of events, we will have a better idea of their long-term viability. The coronavirus pandemic forced millions of people to work from home, and, in general, stay at home far more consistently than they would have otherwise, due to the public lockdowns and businesses being closed to in-person visitations (Sameul, 2021). Because of this, there were far more transactions made online, encouraging digital payment methods, like cryptocurrencies, to be used at a much higher rate. This, combined with the government stimulus payments that were injected into economies around the world, allowed people to not only use cryptocurrencies much more frequently but also allowed many more people to begin using cryptocurrencies as a form of investment. The coronavirus pandemic, along with the responses of governments around the world, ultimately created the perfect storm for cryptocurrency market capitalizations to increase across the board, with cryptocurrencies such as Bitcoin gaining over six times their initial evaluations beginning at the start of the pandemic.

Despite gaining much more popularity than they had before, cryptocurrencies were not able to maintain all of the gains they had amassed from the coronavirus pandemic. At its peak in the final quarter of 2021, a single Bitcoin had a value of USD 65,000, however, as 2022 began, Bitcoin, along with cryptocurrencies across the board, saw a massive drop in value, dropping down to below USD 20,000 (a relative drop of about 70%) for the first time since the start of the pandemic. These massive drops in value are a result of numerous factors, however, the driving

factor behind all of them was the increased interest rates that the United States federal government was rolling out in response to the high inflation at this time, which was surprising for cryptocurrency users as cryptocurrencies, especially those with a limited supply, have been thought of as a hedge against inflation. If we look at other markets, such as the S&P500 index, the relative drop in price was only about 20 percent in this same time span - less than a third of the drop that Bitcoin experienced. Both events show just how volatile cryptocurrency can be - when the economy is doing well, cryptocurrencies seem to do even better, and when economies are falling, cryptocurrencies seem to fall even more. In the last several months, at the time of writing this paper, cryptocurrencies have been trending upward, but are still nowhere close to the evaluations they had during the pandemic in 2021.

Public Opinion

After a series of cryptocurrency exchange collapses, scandals, and bankruptcies, views on cryptocurrencies have changed dramatically in the last year. Although not solely responsible for the shift in public opinion over cryptocurrencies, one of the driving factors for this shift has been the collapse of the popular cryptocurrency exchange, FTX, which was founded by Sam Bankman-Fried. In early November, cryptocurrency news site, CoinDesk, released a report disclosing that the exchange's sister company, Alameda Research, held a position valued at $5 billion in FTT, the native cryptocurrency that was created by FTX. This prompted concern across the cryptocurrency industry about the amount of leverage Bankman-Fried's companies had in FTT. Days later, the world's largest cryptocurrency exchange, Binance, announced that they would sell the entirety of their position in FTT - roughly $529 million, which forced FTX into a liquidity crisis, in which hundreds of thousands of cryptocurrency users tried to pull out their crypto from the exchange, and simply couldn't. Days went by, and more and more people were

unable to pull out their cryptocurrency, which ultimately resulted in FTX filing for bankruptcy, Bankman-Fried stepping down as CEO, and billions of dollars' worth of investors' cryptocurrency being lost (Reiff, 2023).

To see specifically just how much public opinions on cryptocurrency have shifted since the FTX collapse, we can look at the CNBC All-America Economic Survey. In the report, we can see a strong shift in public opinion across all metrics, with the majority of cryptocurrency users now favoring stronger regulations on the cryptocurrency market. The survey found that 43% of the public now hold a negative view of cryptocurrencies, which is up from 25% in March, while the percentage with a positive view plummeted to just 8% from 19%. Even among crypto investors, 42% now have a negative view of the asset, in line with the 43% result for all adults in the survey. The survey also found that 53% of the public believes crypto should have the same or greater regulation and oversight as stocks and bonds (Steveliesman, 2023).

This survey shows a significant decrease in popularity and credibility for cryptocurrencies, which were once endorsed as their asset class and backed by many high-profile public figures, such as celebrities, athletes, as well as other businesses. Now, the same can not be said, as the data suggests that there is not nearly as much support for cryptocurrencies as there was before. This poses a significant challenge for the future and long-term viability of cryptocurrencies, as they inherently rely on the network of users that make them up, both in terms of maintaining the value of the currency, as well as the individuals who contribute their processing power to keep the network alive. As of now, it remains to be seen if cryptocurrencies will be able to gain back the reputation and public support that they once had, as the price of all cryptocurrencies are down tremendously from their peak, and collapses like these only make the situation worse.

Direction Cryptocurrencies Are Heading

Cryptocurrencies have become increasingly popular in recent years, both from the perspective of their users and governmental bodies who wish to regulate them. However, there are undoubtedly many challenges that cryptocurrencies inherently face, such as volatility, security, regulation, adoption, and innovation. Even in the past 10 years, cryptocurrencies have undergone a tremendous amount of change, starting with almost no support from anyone, to now becoming an industry worth trillions of dollars. With this in mind, it is almost impossible to predict the direction cryptocurrencies are headed with absolute certainty, but in this section, we will take a look at 3 different areas in which cryptocurrencies are changing to give us an idea of what we could expect to see in the industry moving forward.

Regulation and Oversight

As cryptocurrency begins to grow even more, it will inherently attract more attention and scrutiny from governmental bodies, as a way to maintain some level of control over these currencies, despite their decentralized nature. Many countries are continuing to pass new laws and regulations that govern the use, taxation, and supervision of cryptocurrencies and their associated activities. For example, in the United States, the Securities and Exchange Commission (SEC) has begun cracking down on unregistered cryptocurrency offerings and platforms such as Coinbase, Binance, and Ripple, arguing that these companies violated securities laws as well as offered unregistered securities products. In general, the SEC has been seen to be taking the security and regulatory efforts associated with cryptocurrency much more seriously, and they are not the only governmental body to do so.

Another organization that has been making strides to regulate cryptocurrency more so than before is the Financial Action Task Force, which has issued global standards for preventing money laundering and terrorist financing involving cryptocurrency assets. These standards require countries to step in and ensure that cryptocurrency service providers such as exchanges and wallet services comply with anti-money laundering and counter-terrorism financing. These standards will be enforced through transaction monitoring, record checks, and more reporting in general. One of the more controversial decisions in these standards is to require cryptocurrency service providers to disclose information about the parties involved in a cryptocurrency transfer, above a certain amount. This is a big deal for cryptocurrency users, as one of the fundamental beliefs of those who use these currencies is their right to privacy, which these standards would limit.

Innovation in Cryptocurrency

Cryptocurrency is a rapidly evolving technology, with innovations in the field being constantly added and improved upon. One of the more popular innovations in the last several years has been the emergence of NFTs - non-fungible tokens, which are a unique type of cryptocurrency that represents the ownership someone has over a commodity, such as art, games, music, sports, and plenty of other applications. What distinguishes NFTs from regular cryptocurrencies is the fact that they are non-fungible, meaning they are not interchangeable and have different values depending on the demand for a given NFT. They have gained vast amounts of popularity in the last year, which has created an entirely new market for artists, creators, fans, and collectors. However, NFTs also pose many of the same risks that traditional cryptocurrencies have, such as regulatory concerns, volatility, and fraud, as they use the same underlying technology that cryptocurrencies use - blockchain. It is important to understand that, although

there is constant innovation in the field of cryptocurrencies, there are still several fundamental problems with this type of technology that have still not been solved.

Risk and Reward - Will It Last?

From its inception, cryptocurrency has been both praised and criticized for the functionality that it offers. Fundamentally, cryptocurrency aims to be an alternative form of currency that takes out the need for intermediaries, such as banks and governments, by distributing the power of the network amongst its users, thereby being completely transparent. To many, this sounds appealing, while others, including banks, governments, and regulatory bodies, they find the inherent decentralized and distributed nature of cryptocurrency concerning for its lack of control and oversight. As it sounds, the spectrum for which people approve or disagree with cryptocurrency is very complex, and answering the question "Will it last?" is not straightforward. To answer this question as accurately as possible, all attributes, risks, and benefits that cryptocurrency offers, must be taken into consideration to produce the most appropriate estimation. This section will focus on determining how each one of these factors will affect the long-term viability of cryptocurrencies, in hopes of giving a more informed answer to this question - "will it last?".

Implications of A Widespread Adoption

Since its inception, cryptocurrency has been a subject of intense scrutiny and debate, and while some believe that it is the future of all currency for the inherent benefits it offers, many also argue that it is a risky, volatile, and, in the long term, a non-sustainable technology. One factor that cannot be ignored when discussing the viability of cryptocurrency in the long term is the potential implications that widespread adoption of the currency would result in. From a

societal, governmental, and economic perspective, the implications that would follow in each of these sections of our society would be significant. In this section, we will explore the potential implications of the widespread adoption of cryptocurrency and what it would mean for the future of our society in each of these areas.

In the last several years, cryptocurrency has grown tremendously, and, as it becomes more widely adopted, the potential implications that it could have on our society are significant. From the societal perspective, it could lead to an inherently more decentralized financial system where individuals are more responsible and in control of their finances while being less reliant on centralized authorities such as banks and governmental bodies. This could lead to overall more financial inclusion, as individuals who may not have equal access to traditional banking institutions would still be able to participate in the economy.

However, more widespread adoption of cryptocurrency could also lead to many negative societal implications, such as increased cryptocurrency-related crime. Due to its decentralized and distributed nature, cryptocurrency inherently makes it easier for criminals to hide their activity, as it is far more difficult to trace these transactions over traditional fiat currency. Take, for example, money laundering. With the current regulations in place, it is very easy for someone to turn their illegally obtained cash into a cryptocurrency like Bitcoin to avoid paying taxes and, or, hiding their money entirely. If cryptocurrency were to become more widely adopted, this is an area that would need to be addressed, as it currently stands to be extremely easy to commit crimes like this, and it would only get worse as more people in our society begin to use cryptocurrency.

From the governmental perspective, the biggest implication of more widespread adoption of cryptocurrency would be the challenges governmental bodies and central banks would face as

a result of this increased adoption. Because cryptocurrency transactions can occur outside of traditional banking institutions, they are not subject to the same regulation and oversight. Some governments see this as a threat to their monetary policy, and could potentially limit the usage of cryptocurrency in their country as a whole by either increasing regulations regarding cryptocurrency or banning the currency entirely.

From an economic perspective, more widespread adoption of cryptocurrency could also have significant implications for traditional banking institutions and the way they function. As cryptocurrency adoption increased in our society, we would see that banks would have a decreased demand for their services, as individuals would no longer need to deal with a centralized authority to oversee their transactions. However, it is also likely that in this scenario financial institutions, such as banks, would begin to invest heavily in cryptocurrency and blockchain technology as a means of keeping their businesses relevant as cryptocurrency adoption increased. This could potentially lead to more economic growth in these sectors, both in terms of the amount of capital allocated to them as well as the number of jobs available.

Overall, the implications of greater adoption of cryptocurrency are extremely complex and nuanced. While it certainly has the potential to revolutionize the way businesses and individuals manage their finances, invest, and make transactions in general, there are also inherently many risks and drawbacks associated with cryptocurrency that must be addressed before even considering this amount of growth in the long term. It will be up to the individual users of cryptocurrencies, governments, and financial institutions to determine how to navigate these risks and find the best path forward for the future of cryptocurrency and related industries.

The Challenge of Regulating Decentralized *Cryptocurrencies*

Before assessing the risks and benefits associated with cryptocurrencies, we must first determine whether or not the fundamental attributes and beliefs associated with cryptocurrencies can coexist with governmental and regulatory bodies in the first place, as they directly have the power to limit those who use them. On one side of the spectrum, countries such as China have directly banned cryptocurrencies like Bitcoin from being used within their jurisdiction for the potential risks that they bring, such as high volatility, lack of control, energy consumption, and cryptocurrency-related crimes like money laundering. On the other side of the spectrum, in countries such as the United States, cryptocurrencies are completely legal, although there are many regulatory measures in place to maintain some level of control over these currencies, despite their fundamentally decentralized and distributed nature.

At the time of writing this paper, there are only a handful of countries, such as China, that have directly banned cryptocurrencies altogether, indicating that the majority of the world's governmental bodies do not have a big enough issue with cryptocurrencies to ban them outright. Instead, most of the world has opted to create more regulatory measures around cryptocurrencies to gain more control over them compared to the little that they had before, due to their decentralized nature. While these measures will allow cryptocurrencies to coexist with governments, these measures will limit some of the fundamental ideas associated with these currencies such as anonymity, security, and a desire for eliminating the need for oversight from a central authority. For cryptocurrency to last into the future, a balance must be struck between the amount of regulatory measures in place, without eliminating their fundamental functionality entirely. As of writing this paper, the public seems to be in favor of this, with over 50% of the United States being in favor of more crypto-related regulations, suggesting that cryptocurrency

users are willing to sacrifice some level of its functionality to provide a more sustainable, and safe network to use cryptocurrency moving forward (Steveliesman, 2023).

Challenges as an Alternative Currency

One of the core reasons cryptocurrencies were developed in the first place was to provide the public with an alternative form of currency. Advocates of the currency believe the benefits the technology brings, such as decentralization, security, and anonymity will eventually allow it to be used in place of traditional fiat currencies, even going so far as to say cryptocurrencies could be used as a hedge against the inflation associated with traditional fiat currencies. However, in practice, neither of these benefits has come to fruition, due to the high volatility that cryptocurrencies experience. For any currency to be seen as legitimate, it must have a stable value that people can quantify when purchasing a commodity. However, not only do most businesses not accept cryptocurrency at all, but the amount of purchasing power that cryptocurrencies have, even with businesses that will accept them as payment, varies tremendously. Traditional fiat currencies such as the Euro or British pound, fluctuate around 0.5% on any given day, with cryptocurrencies commonly fluctuating around 5-10%. This amount of fluctuation makes using cryptocurrency as an alternative payment method essentially impossible, as the amount of buying power that they possess is not nearly consistent enough to justify this use. While this aspect of cryptocurrencies is not holding back their long-term viability entirely, this is an area that will need to be addressed moving forward for cryptocurrencies, as it is one of the main concerns people have when deciding if they should use them or not.

Assessing The Risks of Cryptocurrency

Perhaps the biggest threat to the longevity of cryptocurrency is the inherent risks that come along with them, such as environmental impacts and cryptocurrency crimes. As examined before, the environmental impacts that have resulted from the absurd amount of energy required from these networks are significant, oftentimes being compared to the energy consumption of a moderately sized country. As for cryptocurrency crimes, there are endless avenues in which cryptocurrencies can be leveraged to elicit illegal activity (Chainanalysis, 2022). By their very nature, cryptocurrencies fundamentally lack the oversight that traditional fiat currencies experience, which makes them very beneficial for illegal activities in which adversaries wish to stay anonymous. However, both issues are presently being addressed in hopes of creating a better outlook for cryptocurrencies.

In terms of environmental implications, the cryptocurrency industry has been combatting these effects by working towards adopting more renewable energy sources to power the networks these cryptocurrencies use. For example, more than 200 companies and individuals have pledged to work towards having their cryptocurrency operations become net-neutral by 2030 in terms of carbon emissions through the Crypto Climate Accord (Piven, 2021). This is one of the many different efforts that cryptocurrency users and organizations have been making to address the environmental concerns that the cryptocurrency industry inherently has with the vast amounts of energy being consumed.

As for cryptocurrency crimes, it will be almost impossible to eliminate them without constricting the fundamental functionality of cryptocurrencies entirely. However, regulatory bodies are certainly working towards finding a balance between the two, especially after catastrophes like the FTX collapse. Although not perfect, governmental bodies are constantly

creating new protocols, laws, and guidelines to prevent events as big as FTX from happening, while also aiming to prevent more low-level crimes such as money laundering from being as common.

When assessing the long-term viability of cryptocurrency from the perspective of some of its biggest concerns, such as its environmental impacts and related cryptocurrency crimes, what matters more than both of these issues being resolved in the short term is the direction that governmental bodies are taking to address them moving forward. In the short term, both of these concerns are still very common in the cryptocurrency space, however, it is clear that organizations and governmental bodies are aware of this and are changing their policies, actions, and general goals to be more sustainable in the long run. It is clear from the way that both of these issues are being addressed that cryptocurrency organizations are willing to meet new regulations, policies, and protocols set in place by regulatory bodies to ensure the long-term viability of cryptocurrency.

Chapter 5: Conclusion

While cryptocurrency has many undeniable benefits that are attractive to its users, the viability of cryptocurrency in the long term is simply too complex and nuanced to determine with absolute certainty. Some of the major benefits of cryptocurrencies include decentralization, anonymity, and security, although these benefits alone are not enough to ensure the future of cryptocurrency entirely, as there are many hurdles that cryptocurrencies still need to address moving forward, such as volatility, cryptocurrency-related crimes, government involvement, and energy consumption. However, the direction that the industry as a whole is taking in response to these issues indicates on some level that the sector is willing to adapt to the changing needs of its users and environment. This can be seen in the form of new regulations constantly being implemented by governments who support these currencies, as deemed necessary, in hopes of limiting these aforementioned issues. With this in mind, cryptocurrency will likely be around in some regard in the future, although, with all other factors considered, it is impossible to determine if it will be able to experience the same level of growth as it has in the past or maintain its current level of use with absolute certainty.

Bibliography:

Ammous, Saifedean, Blockchain Technology: What is it Good for? (August 8, 2016). Available at SSRN: https://ssrn.com/abstract=2832751 or http://dx.doi.org/10.2139/ssrn.2832751

Chainalysis. (2023, March 6). *Crypto crime trends for 2022: Illicit transaction activity reaches all-time high in value, all-time low in share of all cryptocurrency activity*. Chainalysis. https://blog.chainalysis.com/reports/2022-crypto-crime-report-introduction/

Carter, N. (2021, May 6). How much energy does Bitcoin actually consume? Harvard Business Review. https://hbr.org/2021/05/how-much-energy-does-bitcoin-actually-consume

Frankenfield, Jake. "What Is Bitcoin? How to Mine, Buy, and Use It." *Investopedia*, Investopedia, 14 Oct. 2022, https://www.investopedia.com/terms/b/bitcoin.asp.

Frankenfield, Jake. (2023a, January 5). *Merkle tree in Blockchain: What it is and how it works*. Investopedia. https://www.investopedia.com/terms/m/merkle-tree.asp

FAUZI, M. A. (n.d.). *Bitcoin and cryptocurrency: Challenges, opportunities and future works*. The Journal of Asian Finance, Economics and Business. https://koreascience.kr/article/JAKO202026061031775.page

Field, M. (2021, January 28). *Inside the dirty world of bitcoin mining*. The Telegraph. https://www.telegraph.co.uk/technology/2021/01/28/inside-dirty-world-bitcoin-mining/

Hayes, Adam. "Blockchain Facts: What Is It, How It Works, and How It Can Be Used." *Investopedia*, Investopedia, 4 Oct. 2022, https://www.investopedia.com/terms/b/blockchain.asp.

IBM."What Is Blockchain Technology? - IBM Blockchain." *IBM*, https://www.ibm.com/topics/what-is-blockchain.

Jara, A. (2022, June 29). *The relationship between Blockchain and cryptocurrency*. GetSmarter Blog. https://www.getsmarter.com/blog/career-advice/the-relationship-between-blockchain-and-cryptocurrency/

Khan, S. N., Loukil, F., Ghedira-Guegan, C., Benkhelifa, E., & Bani-Hani, A. (2021, April 18). *Blockchain Smart Contracts: Applications, challenges, and future trends - peer-to-peer networking and applications*. SpringerLink. https://link.springer.com/article/10.1007/s12083-021-01127-0

Kelsie Nabben Researcher / PhD Candidate. "Cryptocurrency Has an Impact on Economies. That's Why Some Are Afraid of It – and Some Welcome It." *The Conversation*, 4 Aug. 2022, https://theconversation.com/cryptocurrency-has-an-impact-on-economies-thats-why-some-are-afraid-of-it-and-some-welcome-it-175911.

Kuchta, David M. “Why Cryptocurrency Is Bad for the Environment.” *Treehugger*, Treehugger, 10 Sept. 2022, https://www.treehugger.com/why-cryptocurrency-is-bad-for-the-environment-5222940.

Overgaag, Alexandra. “What Is the Economic Impact of Cryptocurrencies?” *Cointelegraph*, Cointelegraph, 14 Oct. 2022, https://cointelegraph.com/explained/what-is-the-economic-impact-of-cryptocurrencies.

Ramaswamy, Anita. (2023, March 24). *Breakingviews - Bitcoin is a solution looking for a problem*. Reuters. https://www.reuters.com/breakingviews/bitcoin-is-solution-looking-problem-2023-03-24/

Reiff, N. (2023, April 23). *The collapse of FTX: What went wrong with the Crypto Exchange?* Investopedia. https://www.investopedia.com/what-went-wrong-with-ftx-6828447

Rodeck, D. (2022, April 28). What is blockchain? - communications.pasenategop.com. https://communications.pasenategop.com/wp-content/uploads/sites/15/2022/06/What-Is-Blockchain.pdf

Rude Baguette. “Opinion: Yes, Crypto Is Crashing Again, but Blockchain Will Survive.” *Rude Baguette*, 19 June 2022, https://www.rudebaguette.com/en/2022/06/opinion-yes-crypto-is-crashing-again-but-blockchain-will-survive/.

Samuel Asumadu Sarkodie, Highlights•COVID-19 effects on cryptocurrencies including Bitcoin, & AbstractThe COVID-19 global pandemic has disrupted business-as-usual. (2021, April 6). *Covid-19 pandemic improves market signals of cryptocurrencies–evidence from Bitcoin, Bitcoin Cash, Ethereum, and litecoin*. Finance Research Letters. https://www.sciencedirect.com/science/article/pii/S1544612321001306

Sergeenkov, Andrey. “How Does Ethereum Work?” *CoinDesk Latest Headlines RSS*, CoinDesk, 7 Sept. 2021, https://www.coindesk.com/learn/how-does-ethereum-work/.

Sharma, T. K. (2022, November 3). *Permissioned and permissionless blockchains: A comprehensive guide*. Blockchain, AI & Web3 Certifications. https://www.blockchain-council.org/blockchain/permissioned-and-permissionless-blockchains-a-comprehensive-guide/

SoFi. “Understanding the Different Types of Cryptocurrency.” *SoFi*, SoFi, 26 Sept. 2022, https://www.sofi.com/learn/content/understanding-the-different-types-of-cryptocurrency/.

Steveliesman. (2022, December 7). *Just 8% of Americans have a positive view of cryptocurrencies now, CNBC survey finds*. CNBC. https://www.cnbc.com/2022/12/07/just-8percent-of-americans-have-a-positive-view-of-cryptocurrencies-now-cnbc-survey-finds.html

Tut, Daniel, Bitcoin: Future or Fad? (March 20, 2022). Tut, D. (2022). Bitcoin: Future or Fad? In: Walker, T., Davis, F., Schwartz, T. (eds) Big Data in Finance. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-031-12240-8_8, Available at SSRN: https://ssrn.com/abstract=4168188