iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** VI **Month of publication:** June 2022

DOI: https://doi.org/10.22214/ijraset.2022.43812

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VI June 2022- Available at www.ijraset.com

Cryptocurrency: The Present and the Future Scenario

Anusha Ramkumar Kommuru[1], Aastha Gupta[2], Manvi Chauhan[3]
[1, 2, 3]*UG Student, Department of Computer Science, Dronacharya Group of Intuitions, Greater Noida, India*

Abstract: ***Cryptocurrency is a digital means of exchange of non-physical or digital currencies. It is a universal currency system which resolves the problem of currency exchange between two different nations with different currencies. Thus, cryptocurrencies have risen as imperative financial software systems in various countries. It is dependent on a secure distributed ledger data structure for the transactions. The exchange rates on the cryptocurrencies are not stable and keep changing with time, thus it is exploited the most by the traders. Mining is a method through which new units of cryptocurrencies are generated and earned. It also adds past transactions to the distributed and open ledger among the users known as the blockchain.***
In this paper, we shall discuss the mining techniques, growth of cryptocurrencies and the associated risks and returns.
Keywords: Types of cryptocurrencies, Mining, Factors of its growth, Risks and returns, Challenges and problems

I. INTRODUCTION

A cryptocurrency, crypto-currency, or crypto is a digital currency designed to work as a medium of exchange through a computer network that is not reliant on any central authority, such as the government or bank, to uphold or maintain it.
Coin ownership records are stored in a digital ledger, which is a computerized database using strong cryptography to secure transaction records, control the creation of additional coins, and verify the transfer of coin ownership. Cryptocurrency does not exist in physical form and is typically not issued by the central authority. It typically uses decentralized control as opposed to a central bank digital currency(CBDC). When a cryptocurrency is minted or created before issuance or issued by a single issuer, it is generally considered centralized. When implemented with decentralized control, each cryptocurrency works through distributed ledger technology, typically a blockchain that serves as a public financial transaction database.
A cryptocurrency is a tradable digital asset or digital form of money, built on blockchain technology that exists online. Cryptocurrency uses encryption to authenticate and protect transactions hence the name. There are currently over a thousand different cryptocurrencies in the world.
Bitcoin, first released as open-source software in 2009, is the first decentralized cryptocurrency.

A. History

Many think cryptocurrency is a concept developed and launched in the last decade or so, but the history of cryptocurrency reaches as far back as 1983. These virtual coins can be traced back to one man: cryptographer David Chaum.
Chaum developed the first brand of digital currency with a transaction system called eCash, which was followed by another iteration of the same principle a few years later with DigiCash. The foundational element of DigiCash is that transactions were anonymous and conducted over a public network.
PayPal is an Online Money Transfer System established in 1998. It provides users with an account, which can be linked with bank accounts and credit cards, and users can pay someone or receive payment through PayPal accounts. It doesn't have its currency.
Although the concept of electronic currency dates back to the late 1980s, Bitcoin, launched in 2009 by pseudonymous developer Satoshi Nakamoto is the first successful decentralized cryptocurrency. In short, we can say cryptocurrency is a virtual coinage system that functions much like a standard currency, enabling users to provide virtual payment for goods and services free of a central trusted authority.
It relies on the transmission of digital information, utilizing a cryptographic method to ensure legitimate, unique transactions. Bitcoin took the digital coin market one step further, decentralizing the currency and freeing it from hierarchical power structures. It caught wide attention in 2011, and various altcoins – a general name for all other cryptocurrencies post – Bitcoin – soon appeared.
Litecoin was released in the fall of 2011, gaining modest success and enjoying the highest cryptocurrency market cap after the Bitcoin unit was overtaken by Ripple on October 4th, 2014. Litecoin is used to script sistahs functions instead of SHA-256.

Litcoin modified Bitcoin's protocol, increasing transactions. Another notable cryptocurrency, Peercoin, used a proof-of-work/proof–of–stake hybrid. Ripple launched in 2013, introduced a unique model to that used by Bitcoin and currently maintains the second-highest market capitalization.

In June 2021, EI Salvador became the first country to accept Bitcoin as legal tender, after the Legislative assembly had voted 62-22 to pass a bill submitted by President Nayib Bukele classifying the cryptocurrency as such.

In August 2021, Cuba followed with Resolution 215 to recognize and regulate cryptocurrencies such as bitcoin.

In September 2021, the government of China, the single largest market for cryptocurrency, declared all cryptocurrency transactions illegal, completing a crackdown on cryptocurrency that had previously banned the operation of intermediaries and miners within China.

B. Basic Terminologies

1) Blockchain

Every cryptocurrency transaction is processed, verified, and recorded on a virtual ledger known as a blockchain. When someone buys or sells using cryptocurrency, another entry is made on this virtual ledger.

Think of the blockchain as a series of boxcars from a train. When a cryptocurrency transaction is made, another boxcar is added to the train. The blockchain is decentralized. This means it's not stored on one machine or even across one network. Instead, the blockchain exists on computers all over the world that are accessible because of the internet. People and companies help verify each transaction that gets added to the blockchain using their own computer's processing power on a decentralized peer-to-peer network. Each transaction is timestamped, individually encrypted, and cannot be reversed or changed.

2) Flat

Cryptocurrency, on the other hand, is virtual money. Cryptocurrencies are not backed by governments or any other standard used with traditional currency. Each "token" represents the amount you own. Each token worth varies based on the current market value. One day it's up; the next day down. With cryptocurrency, the price fluctuations can happen much faster and are more extreme- both positive and negative. A good resource to check the current prices is CoinMarketCap.

3) Altcoin

An altcoin is any digital currency that's not Bitcoin. There are thousands of cryptocurrencies, with new ones added all the time.

These are the five currencies with the highest market caps. Since crypto moves so fast, this list may have already changed by the time you're reading.

a) Bitcoin
b) Ethereum
c) Binance Coin
d) Tether
e) Solana

4) Exchange

To buy cryptocurrency, you need to start with an exchange. Think of exchange like a crypto middleman. It's an online service that allows you to exchange your falt or crypto or change crypto into flat.

If you're familiar with traditional investing, a crypto exchange functions as a brokerage. You can deposit money through a bank transfer, by wire, through a debit card, and other standard deposit methods. You can expect to pay fees for most transactions.

You can also buy crypto through apps you already might be using, like Venmo, Robinhood, or Cash App.

5) Wallet

In basic terms, a cryptocurrency wallet is an app or physical storage device that allows you to store and retrieve your digital currency. Wallets can hold multiple cryptocurrencies, so you're not limited to just Bitcoin, for example.

Whether you use an app or a physical wallet, it's important to note that the currency itself isn't stored there. Rather, wallets store the location of your currency on the blockchain.

Wallets are split into two main categories: Hot and cold. A hot wallet is, by definition, connected to the internet. The most secure way to store your cryptocurrency is with the cold wallet- one that isn't connected to the internet. Physical wallets come in different types but are usually specially designed USB drives that directly store your cryptocurrency for later use. Physical wallets provide you with the most protection from hackers.
Two popular cold wallets are the Ledger Nano X and Trezor Model One. Of the two, prefer the Ledger Nano X because it supports 23 different types of cryptocurrencies and has additional features.

6) Mining
You have probably heard this term associated with Bitcoin, which is created by mining. Computers mine coins by solving complex math problems. The more powerful the computer, the faster it can "think".
Now if your computer is the fastest one to solve the problem, bingo- you win one unit of whatever cryptocurrency you're mining. While there are a few cryptocurrencies out there with an infinite supply, most have a limit. For Bitcoin, that limit is 21 million. The last coin will be mined in 2140 or sooner.

7) DeFi
Here's another simple one. DeFi is a shortened version of decentralized finance. This term refers to financial transactions that happen without a "middle man," like the government, a bank, or other financial institutions.

8) NFT
Nonfungible tokens, that's a fancy way of saying, "This digital item is one of the kind and irreplaceable." It applies to anything you can imagine, from online artwork to songs, viral videos, articles, text logos, and GIFs. Now any digital item also can be turned into a collectable. They also act as status symbols online. For example, the Twitter profile picture of Jimmy Fallon.
The only way to buy an NFT is by using cryptocurrency. You can buy an NFT through an auction platform, secondary marketplace, or by participating in a mint.

9) Mint
Minting is how a file, such as JPEG or GIF, is recorded to a blockchain. After an NFT is minted, it can be sold or traded. During the minting process, the creator specifies the royalties they receive from future sales. This acts as commission if the work changes hands in the future and is a big draw for artists looking to go digital. If you sell an NFT on a secondary marketplace, it likely gets a cut of the sale too.

10) HODL
This term you might see on social media. HODL stands for "hold on for dear life". Some say it originated as a typo of the word "HODL" on a Bitcoin forum way back, but now it's everyday slang.
The idea behind it is simple: If you believe a project or currency will gain more value, just "HODL" even through dips in the market. Want to dive even deeper, we can use " Cryptocurrency 101", the guide for selling and buying.

C. Types of cryptocurrencies
We can categorize these cryptocurrencies into four types :
(i) Transactional or Payment Cryptocurrencies
(ii) Platform or Infrastructure Cryptocurrencies
(iii) Utility or Financial Cryptocurrencies
(iv) Entertainment and Media Cryptocurrencies

1) Transactional or Payment Cryptocurrencies
As the name suggests, these assets are mainly for payments and are hence called Payment Currencies. For example, you could use payment currencies to pay for goods or services, pay your bills, cash out from digital currencies to local flat currencies like the dollar, etc.
While buying and selling on the cryptocurrency market is becoming increasingly mainstream, the opportunities to spend virtual currencies are somewhat limited in comparison due to their volatility. Some transactional cryptocurrency properties are:

When it comes to cryptocurrency transactions, there are several elements which must be considered. The first hallmark of crypto transactions is that they are irreversible once they have been confirmed and added to the blockchain. There is no way to take back confirmed transactions, this means that once you have sent money to someone else with crypto, the transaction is final. It does take some time for transactions to be confirmed, but this period is growing shorter as new technologies are introduced.

The irreversible nature of cryptocurrency means that individuals must take more care in using digital tokens. Let's contrast using crypto to pay for goods and services with a traditional payment processor like PayPal. When one makes a payment with PayPal to someone they do not know there may be some buyer protections offered in certain cases. An obvious example of this would be a purchase made with eBay. Even after the money has been sent to another party the sender could file a claim if they did not receive their goods.

There are many cryptocurrencies out there in the crypto market. Out of all Bitcoin is the most popular and the most expensive one. But the transaction speed of this coin is slow compared to others. Because of the high transaction speed, some cryptocurrencies are effective.

Ripple or XRP: This coin is released in 2012 by Chris Larsen and Jed and is to be referred to as the nest digital asset for worldwide payments. The official website of Ripple says that it provides smooth digital payments and gives a global economic opportunity. The payment with Ripple assures an open-source, decentralized, and peer-to-peer network that supports seamless transactions.

It is one of the fastest and the most secure blockchains one can find in the crypto exchange which can process 1500 transactions in just 3-5 seconds. Also, at the same same time, it records it in the blockchain ledger too.

For example, let us consider a bitcoin transaction between a user and a merchant. Suppose a user owes the merchant 2.5 BTC for a certain service he had provided. Now, if the user has 0.5 BTC in his/her wallet, the amount cannot be broken down. The entire amount gets deployed in the transaction 0.25 goes to the merchant and the rest of 0.25 goes to a new account that the bitcoin wallet creates to receive the change from the merchant.Although the process may sound complicated, one has to remember that creating a new address to receive the change is not something that the user has to do. It happens automatically through the user's wallet.

We discussed bitcoin's transaction fee as an example. There are many other cryptocurrencies available in the market with a wide range of transaction fees. Some of them are beneficial to accept as payment. Here, we will discuss the issue of the cryptocurrency transaction fee or blockchain transaction fee a bit more.

Some of the popular platforms are often the ones that have comparatively higher transaction costs. This is because the miners are well aware of how important these platforms, such as Bitcoin and Ethereum, are for the business and customers habituated with crypto transactions. Therefore, the miners enjoy an edge in terms of asking for a higher rate to validate and verify transactions in these exchanges.

Fig: 1 Transactional and payment cryptocurrency

2) Platform or Infrastructural Cryptocurrencies

Infrastructure cryptocurrencies are typically used to pay the computers responsible for running programs on a shared blockchain software network. For example, the crypto asset that powers Ethereum is called ether, and it may be considered an infrastructure cryptocurrency, as people must purchase it to create and use decentralized applications running on the network. Many blockchain platforms provide different use cases, and each of them requires its infrastructure of cryptocurrency. Just to name a few examples: Ethereum Classic(ETC), Tron(TRX) and EOSIO (EOS).

Below we've listed 4 Crypto that is used or intended to be used for platform and infrastructure.

a) Ethereum (ETH)

Ethereum was created in 2014 by Vitalik Buterin. It is the second most capitalized cryptocurrency on the market, behind Bitcoin. At first glance, Ethereum's blockchain works on the same model as Bitcoin's since it is based on the open-source principle and requires computing power from computers to validate transactions, which is called proof of work. The Ethereum network is also decentralized.

Ethereum has pioneered the concept of blockchain smart contract platforms. Smart contracts are computer programs that automatically execute the actions necessary to fulfil an agreement between several parties on the internet. They were designed to reduce the need for trusted intermediates between contractors, thus reducing transaction costs while also increasing transaction reliability.

Ethereum's principal innovation was designing a platform that allowed it to execute smart contracts using the blockchain, which further reinforces the already existing benefits of smart contract technology. Ethereum blockchain was designed according to the co-founder Gavin Wood, as a sort of " one computer for the entire planet," theoretically able to make any program robust, censorship-resistant and less prone to fraud by running it on a globally distributed network of public nodes.

b) Binance coin (BNB)

BNB is the native token of Binance Smart Chain and Binance Chain. First minted in July 2017 on Ethereum. BNB is a utility token that allows holders to pay discounted fees for trading on Binance's exchange. Binance coin initially ran on the Ethereum blockchain with ERC 20 standard but has since become the native coin of the Binance chain. It was launched during an initial coin offering (ICO) in July 2017 and has a strict maximum of 200 million BNB tokens.

As of June 2021, Binance Exchange is the largest Cryptocurrency exchange in the world, supporting more than 1.4 million transactions per second. It offered 10%, or 20 million, BNB tokens to angel investors, 40% or 80 million, tokens to the founding team, and the remaining 50%, or 100 million, to the various participants through the ICO process.

Every quarter, Binance uses one-fifth of its profits to repurchase and permanently destroy, or "burn", Binance coins held in its treasury. The crypto token has gathered support from other partnerships with Asia's premier high-end live video streaming platform, Uplive, which sells virtual gifts for BNB tokens to Uplive's 20 million-strong user base. Binance coin is also supported by the platforms, the mobile app, the VISA debit card of Monaco, the pioneering payments and the cryptocurrency platform.

Fig: 2 Binance coin

c) Cardano (ADA)

Cardano is a blockchain network with a Proof of Stake consensus mechanism. The project was created in 2015 by Charles Hoskinson, a co-founder of Ethereum. The open-source project also aims to "redistribute power from unaccountable structures to the margins to individuals" – helping to create a society that is more secure, transparent and fair.

Cardano was founded back in 2017, and named after the 16th-century Italian polymath Gerolamo Cardano. The native ADA token takes its name from the 19th-century mathematician Ada Lovelace, widely regarded as the world's first computer programmer. The ADA token is designed to ensure that owners can participate in the operation of the network. Because of this, those who hold the cryptocurrency have the right to vote on any proposed changes to the software.

In 2020, Cardano held a Shelley upgrade that aimed to make its blockchain "50 to 100 times more decentralized" than other large blockchains. At the time, Hoskinson predicted that this would pave the way for hundreds of assets to run on its network. The Alonzo hard fork launch in September 2021 will bring an end to the Shelley era and the usher in the Goguen phase. Users can develop and deploy smart contracts on Cardano, allowing native decentralized applications (DApps) to be built on blockchain. Cardano's price broke the $3 mark and hit an all-time high of $3.101 on Sept. 2, 2021, ahead of the launch.

Fig : 3 Cardano coin

d) Solana (SOL)

Solana is a decentralized protocol for building dApps with a reported throughout of 65000 transactions per second (TPS) thanks to its distributed computing system. Unlike most protocols that run with the Proof of Stake (PoS) or Proof of Work (PoW) mechanism, Solana uses the Proof of History (PoH)- a new cryptographic mechanism that amplifies scalability while maintaining network security.

POH relies on Proof of Stake, using the Tower BFT algorithm for consensus, which functions as an additional tool to verify transactions. At its core, PoH is a high-frequency Verifiable Delay Function(VDF). A VDF is a triple function (Setup, Evaluation, Verification) to produce a unique and trustable output. It maintains order in the network and can move forward.

In Solana cases, it uses SHA256 (secure hash algorithm 256-bit) -a set of patented cryptographic functions that output a value 356 bits long(which is also the one bitcoin uses). The Solana network periodically samples the count and hashes of the SHA256, providing real-time data instructed by the set of hashes included on the CPU.

Validators can use this sequence of hashes to record a specific piece of data created before a particular had index is generated. The timestamp for transactions is generated once this piece of data is inserted. The project debuted via an initial coin offering (ICO), raising over $25.6 million in march 2020. In June 2021, however, Solana labs also raised $314 million for further development of the network. Since then, it has become one of the fastest-growing protocols DeFi space. In 2021, the protocol got the market attention not because of its technology but because of the impressive performance of its native SOL token which exploded in value.

3) Utility or Finance Cryptocurrencies

Utility tokens are digital tokens that are used for a blockchain-based product or service. They run on a blockchain platform, or in other words, are part of a Blockchain Economy. Most utility tokens are ERC20 tokens that run on the Ethereum blockchain but with the continued release of other blockchain platforms. Other token types like TRC10 and TRC20 tokens have emerged as well. Utility cryptoNeon(NEO)employs an algorithm that runs on a proof of stake decentralized Byzantine fault-tolerant (dBFT)consensus mechanism between several centrally approved nodes.

a) Polkadot (DOT)

The Polkadot network includes a main blockchain called the 'relay chain' and many user-created parallel chains. It also has a connecting layer, or "bridge", that allows value and data to be transferred between most blockchains and can even be used to connect the non-blockchain database.

In Polkadot Validators do the most work – it's a major commitment, and requires technical know-how. To become a validator, you need to run a node (one of the computers that make up the network) with little to no downtime and stake a substantial amount of your DOT. In exchange, you get the right way to verify legitimate transactions, and new "blocks" of transactions to the relay chain, and potentially earn newly created DOT, a cut of transaction fees, and tips.

Nominators allow regular investors to participate in stalking indirectly. You can delegate some of the DOT validators you trust to behave according to the rules. In exchange, you get a cut of DOT earned by your chosen validators. Be careful with whom you choose: you also can forfeit some of your stakes if your validator breaks the rules.

Two specialized roles typically require less of a commitment than becoming a full validator but more technical skill than is required to be a nominator. Collators keep track of valid para chain transactions and submit them to the relay chain of validators.

4) Entertainment and Media Cryptocurrencies

Cryptocurrencies have the potential to transform several markets within media and entertainment, particularly those where participants would benefit from the security and transparency that blockchain would offer, such as distribution of payments, funding, monetization and contract enforcement.

Blockchain technology is still in the stages of development, but given the excitement around the many ways it could be put to use, it's not too soon for media and entertainment companies to start thinking about the possible implications for their business and the industry as a whole.

a) Basic Attention Token (BAT)

The Basic Attention Token (BAT) was created by the co-founder of Mozilla and Firefox, Brendan Eich, to improve the security, fairness, and efficiency of digital advertising through blockchain technology. It is the native token of the Brave web browser built on top of Ethereum (ETH). BAT's white paper is dated Feb. 10, 2021. As of 2022, the project is still being developed, although the Brave browser is available for download. As of Feb. 11, 2022, there are 54.5 million monthly active users and 16 million daily users of the Brave browser. Bat Token Value: According to its white paper, the Basic Attention Token launch aimed to raise a total of $24 million.[7] The token reached its all-time high in late November 2021, trading at around $1.76 at its peak. As of Feb. 12, 2022, it has a circulating supply of 100%, with 1.50 billion BAT in circulation and a total supply of 1.50 billion BAT.[8]

The exchange rate for BAT is set at 6,400 BAT per ETH, meaning that as the price of Ethereum climbs or falls, the price of BAT will be adjusted proportionally as well.[3] As of Feb. 12, 2022, the exchange rate is 3,628 BAT per ETH.

II. MINING TECHNIQUES

Mining is a process through which each transaction between a payer and a payee is validated and added to a public ledger which is a secure system and distributed among all the users. This public ledger is known as Blockchain. A miner is a person who receives payment for the services rendered by him/her to mine a node. When a new transaction takes place, the role of the miner is to verify whether the currency is owned by the payer or if the payer intends to double-spend [1].

The blockchain also records the ownership of the currencies. An unauthorized user might want to validate an invalid transaction by generating and adding multiple nodes. Thus, to prevent invalid transactions from getting recorded, the miners are required to accomplish a resource-intensive task. Adding these tasks before the actual transaction takes place makes it difficult and more expensive for an unauthorized user to generate enough false identities to exceed the number of genuine users and validate an invalid transaction.

The following may be regarded as the resource-intensive tasks:

- *Proof of Work [2]* is a result of the resource-intensive task that can be used to ensure that the task has been performed with a valid output.
- *Proof of Stake [3]* is used to describe the amount of currency the miner owns.
- *Proof of Retrievability [4]* is used to ensure that the data that was provided to the miner is undamaged and can be retrieved whenever required.

Any type of proof construction demands high computational power and/or memory space. The proof construction bounds the number of transactions that can be validated in a system in a given time interval. The foundation has its significance in the process of mining. If there were no boundaries to the number of blocks that are added to the blockchain, then each block which is mined would subsequently produce a new currency (the total of which is finite). This would help in preventing the exhaustion of the finite amount of the currency reserve available. Once the limit is reached, the number of bits that make up a Bitcoin could be increased to generate more units.

The steps involved in the mining process are as follows:

- A miner is required to produce a Proof-of-Work (PoW) to support the validity of the solution to the resource-intensive task and to segregate himself/herself from the malicious miners who produce invalid transactions.
- The Proof-of-Work (PoW) is verified with the desired output to confirm that the task has been accomplished.
- The miner then has to verify the validity of the transactions contained in the block, and if all of them are proved valid, then the new block is added to the blockchain.

Mining is a hit and trial paradigm which is designed in such a way that the main aim of the process is to keep the number of blocks produced per day constant (or nearly constant), which will consequently lead to lesser unboxing of new currencies from the currency reserve. The first miner who computes the proof earns an opportunity to validate the block and subsequently earns the associated reward for the task.
Cryptocurrencies are mined with one-way functions such as hash functions [5]. The input in these functions is the previous hash of the blocks mined. The miner is required to choose a nonce such that when the nonce and the current hash are hashed, the result is in the form of a structural cryptocurrency model.
Evaluating an input from the hash requires the deployment of a lot of resources whereas validating the hash by calculating the hash block is quite easy and fast. Hash functions are made in a way that consumes the maximum time in turning the input into an output. The miner has to generate nonces and form combinations with the inputs to perform hashing on the combinations until the desired output is produced. The reverse hashing function is harder to compute as the computation of the hash function is a brute-force algorithm. Obtaining the correct nonce and the input combination along with the deployment of numerous resources is quite time-consuming.

A. Mining Methods

1) Bitcoin

Bitcoin mining uses Proof-of-Work (PoW) algorithm which is known as hashcash [6]. In hashcash, the hash algorithm used is SHA-256, which requires the miner to find a suitable nonce which collaboratively hashed with the previous inputs and produces a hash with a defined number of zeroes at its front [6]. The number of zeroes defines the measure of difficulty. The SHA-256 hash of a block's header has to be lower than or equal to the target for the block to be accepted by the network [7].
Bitcoin mining follows the following steps:

- A miner picks a transaction which he/she wants to verify.
- The transactions are then used by the miner to build a Merkle Tree (It is a data structure in which every "leaf" is labelled with the cryptographic hash of a data block, and every node that is not a leaf is labelled with the cryptographic hash of the labels of its child nodes)
- Then the miner generates and adds the nonce and hashes the block header.
- The nonce is incremented and hashing is done until the desired output is produced.
- The result produced after hashing is known as the Proof-of-Work (PoW) which others verify for matching with the correct output. After the verification of the PoW, the transaction is validated and new currencies are floated.

Mining of coins using the SHA-256 hash algorithm requires hash rates in the gigahashes per second (GH/s) range or higher [8]. The current average time needed to mine a Bitcoin Block with SHA-256 is ten minutes [5].

2) Litecoin

Litecoin uses Scrypt for mining, which is a key-derivation function [9]. It was developed by Cervical and published in 2012. Scrypt features the time-space trade-off, which helps in securing the system. For instance, if an attacker tries to forge the system, he/she will require a large amount of memory to attack the system in less time. Scrypt's memory requirement is quite expensive thus making it difficult to perform an attack. Scrypt can be implemented as a Proof-of-Work verification with ease; Litecoin made it possible!

In Scrypt, the large vectors of pseudo-random bit strings demand a huge memory to complete the process faster. After the generation of the vectors, the elements are traversed in a pseudo-random order which combines to generate the drive key. The derive key has predefined characteristics and the miner produces the sequence of bit strings that are matched with the key.

Scrypt is a more secure algorithm than the SHA-2 series. SHA is computationally intensive while Scrypt is memory intensive [10]. The hash rates of Scrypt for successful mining ranges from kilo hashes per second (KH/s) or mega hashes per second (MH/s) degrees of difficulty. Scrypt takes about 2.5 minutes to mine a block with the same difficulty measures.

3) Peercoin

Peercoin uses Proof-of-Work (PoW) and Proof-of-Stake hand-in-hand in the main mining system. In its Proof-of-Work, it uses the double-SHA-256 algorithm [3]. Proof-of-Stake tries to ensure that there is no falsified or duplicate currency being circulated (also referred to as double spending). It requires the Proof-of-stake system to be used by the prover (or the miner) to prove the ownership of a certain amount of currency, rather than requiring the miner to compute the work. In this way, the miners protect their stakes. Proof-of-Stake defines the resources that are equivalent to the amount of the currency a miner holds [3].

Proof-of-Stake requires less energy to accomplish the task. It follows the block selection policy, which includes the following:

- Randomized block selection
- Coin-age based selection
- Velocity based selection
- Voting based selection [11]

Proof-of-Stake is sensitive to the Nothing-at-Stake problem, in which the miners are left with nothing to lose (at stake) if they vote for an invalid transaction [11].

4) Ethereum

Ethereum was crowdfunded in 2014 [12]. Ethereum also uses the Proof-of-Work but it does not use a previously known hash algorithm [12]. A new hashing algorithm exclusive to Ethereum was developed, named EtHash [12, 13].

To scale down the problem of mining centralization, the new Proof-of-Work function was developed by the designers, in which micro-level hardware companies or mining operations hold the power to acquire an uneven proportion of resources to affect the network. EtHash is ASIC-resistant and has the property of relying on how efficiently the memory can transfer the data (also referred to as memory hardness) [13].

5) Ripple

Ripple uses a trust-based system to attain consensus rather than mining [14]. The objective of the consensus is for each server to apply the same set of transactions to the current ledger. The last closed ledger of the system contains the previous transactions and the Ripple accounts used in the previous transactions while, on the other hand, a new ledger is generated in an interval of a few seconds.

A transaction comprises a change in the ledger which can be made by any server in the network. The consensus is aimed to generate a new last closed ledger [14].

6) Namecoin:

*N*amecoin was introduced as the first form of Bitcoin. It uses the same code and the mining algorithm as Bitcoin, instead of having its own. But the difference arises in the storage of data. Namecoin can store data in its Blockchain Transaction Database [15], whereas Bitcoin Blockchain displays valid transactions only (the associated data is stored in a separate database).

7) Auruoracoin

Originating from Iceland, it uses Scrypt as its mining algorithm.

8) Blackcoin

Blackcoin deploys a phenomenon called minting, wherein, it uses Proof-of-Stake independent of the Proof-of-Work. It completes the process in less time as compared to other systems using the Proof-of-Stake systems.

9) Dash

Darksend is a system used in Dash that is used for transaction privacy. Dash differs from other cryptocurrencies by the fact that the transaction information is not available to anyone and everyone. The Proof-of-Work algorithm used in Dash is X11, which is a chained hashing algorithm. It is considered to be more energy efficient when compared with Scrypt [16].

10) Decred

Decred involves the use of a combined system of both Proof-of-work as well as Proof-of-Stake wherein both miners and voters need to achieve the consensus together. The mining algorithm used in Decred is Blake 256 which is a cryptographic hash function based on the ChaCha stream cypher [17].

11) Permacoin

Currently, Permacoin has no practical implementation, but it introduces an entirely new concept of Proof-of-Retrievability [4]. This system demands the miner to store some useful information and generate proof to the verifier of its existence. Permacoin requires a large memory capacity. To secure a cryptocurrency network, storage is preferred to be used above the CPU cycles, which aids in providing an efficient way of data backup. Instead of consuming cycles through Proof-of-Work, which has no intrinsic value beyond the proof itself, Miller et al want miners t store pieces of a large archive of data that is worth preserving [4]. This can be achieved by requiring the miners to prove that they are storing the data. Miners will still have to prove that they have solved a mathematical problem but it will be less computationally expensive, and this process is known as a scratch-off puzzle [4].

The scratch-off puzzle is based on the Floating Pre-image Signature [4]. The miners are required to refer to a section of code stored locally on their device to solve the puzzle. The algorithm results in proving that the miners have stored the data once the miner solves the problem. All miners are thus required to store a piece of the archived data to get involved in mining Permacoin.

III. GROWTH OF CRYPTOCURRENCY AND ITS FACTORS

In the last decade or so we have seen a huge rise in the popularity of digital currencies such as bitcoins, Litecoin, ethers, etc. the growth is mainly seen in developed countries as they are more open to change and adaptability. Companies can take huge advantage of fluctuating cryptocurrencies' prices to strengthen their digital assets.

An example of the adaptability to the easy and flexible methods of transactions that cryptocurrencies have to offer is Facebook. Inc (now known as META) in 2019 had started its digital currency named Libra. Libra can be used to cash in or out the currency in grocery stores or online.

The global cryptocurrency market is projected to grow from $910.3 million in 2021 to $1,902.5 million in 2028 at a CAGR of 11.1% in the forecast period, 2021-2028. [18]

A. Factors for the growth of cryptocurrency:

Though there has been a growth in the popularity of cryptocurrencies, however, its path has been turbulent. Though many argue that its performance has been underwhelming in comparison to its first stir around the market in 2009 [19].

There are mainly two factors that affect the growth of cryptocurrencies which we will discuss in this section. These factors affect the growth of the specific industry and will continue to influence its development and integration into the broader financial scheme well into the future.

B. Government Regulations

Though cryptocurrencies are expanding in their market as they carry the potential to revolutionize the transaction methods, their acceptance has come with many pitfalls. Digital money is not considered the official means of paying off goods and services and hence its growth is slowed. For the currencies to act as a sustainable method of transaction it is required to obtain legal status.

The regulatory systems are expanding in numerous ways by the governments of various countries; however, their current currency systems are still on the run and continue to evolve. The regulations set by the governments will help offer legitimacy at greater rates. Cryptocurrencies are mostly known for transactions during cyber-crimes; hence the government's regulations will help to limit fraud, protect consumers, respect economic sanctions and institute viable taxation methods [20]. The US has taken a permissive neutral state on cryptocurrencies. Their current laws allow them to accept the unique aspects and challenges of virtual money. For taxation purposes, virtual money will be seen as property and will abide by the same taxation norms rather than currency. The Financial Crimes Enforcement Network (FinCEN) has taken the forefront in implementing regulatory methods. They announced in 2013 that the individual use of virtual money shall not be considered a money service business (MSB) however, the exchanges and conversion of the virtual money shall be MSB [21]. There are strict rules placed by the government to add another layer against security fraud, this also demands accountability. The virtual currency transmitters must follow the government requirements established for MSB along with keeping a close record of all transactions and abiding by the Bank Secrecy Act of 1970. For other jurisdictions like the European Union or the UAE, they have proposed new regulations to deal with the industry comprehensively. The indifferences amongst territories can create uncertainties and increase the burden on the business operating sectors [22]. To ensure the growth and use of virtual money, countries should work together to come to a common ground which will help establish a strong set of regulations for safer operations of cryptocurrencies and to meet the objectives set for them.

C. Public Perceptions

The essential value of cryptocurrencies depends upon their number of users. The growth in users depends upon the public trust in virtual memory, using virtual money as an alternative method isn't sustainable. In the recent events regarding the volatility of cryptocurrencies, it has become more difficult to assure the sceptical public that digital currency is the safest transaction method. Hence educating the public and assurance is much needed.

Though there may be negatives with cryptocurrencies, on the latter we have seen many individuals or companies make it big with virtual money by investing, hence they are slowly gaining a global presence in the market. Through a survey conducted in April 2015 by Coincenter.com, it was identified that on average a person is largely unaware of bitcoins (bitcoins were used as a subject as they are more prominent cryptocurrencies), and only 4.5% of the people surveyed had ever used cryptocurrency [23].

D. Consumers and Transactions

Cryptocurrencies are an emerging concept hence it becomes harder to gauge public perception due to the levels of risks involved and the numerous factors that are involved within it. In the cryptocurrency industry, the three largest indicators of success are market capitalization, the estimated number of cryptocurrency users, and daily transaction volume. The rates of success or failure play a huge role in shaping an opinion on something. The above-discussed factors of success help with market capitalization and define the legitimacy of the system. As the number of consumers increases, this metric can act as a factor to attract more.

Due to the user's discrepancy, it is hard to get an exact number of users for bitcoins but by getting a rough estimate of the number of wallets created we can identify the no of users. As of May 2015, the number of Bitcoin wallets created in My Wallet is approximately 3.3 million. The number of wallets increases by approximately 5,000 wallets per day in April 2015[24]. However, it is not an exact number as there may be a single user with multiple wallets necessarily not containing any bitcoins in it.

E. Retailers

Taken over a decade since bitcoins have emerged many large retailers have started accepting payments through bitcoins for example TigerDirect, Overstock.com, and Zanga [25]. On the other hand, the fear of cybercrimes has caused many companies, including banks, to reject the embedding of cryptocurrency systems. Due to the factor that these systems run on proof rather than trust, it becomes a concern amongst many financers as the latter was substituted by cryptographic proof mechanisms. other concerns follow like the possibility of fraud, price volatility, settlement risks, disregard of security, the recent cases of bankruptcy etc.

IV. RISKS AND RETURNS

A. Risks

For the risk factors, we choose the CAPM, Fama French 3-factor, Carhart 4-factor, Fama French 5-factor, and Fama French 6-factor models. The alphas for all of the considered models are statistically significant. The unconditional alpha of the period is 22.45 percent per month. The CAPM adjusted alpha decreases to 18.91 percent per month – a reduction of about 16 percent. The CAPM beta is large at 3.34 but not statistically significant. The beta is statistically significant at the 10-percent level only for the 5-factor and 6-factor models.

The corresponding alphas are 16.72 and 15.98 per cent per month. The exposures to the other factors are not statistically significant. The exposures to the SMB factor are not stable across the specifications: both the magnitude 9 and the signs change when 5-factor and 6-factor models are considered. The exposures to the HML factor are negative and have consistent magnitudes and signs; this suggests that Bitcoin returns may comove more with growth rather than with value firms. The exposures to the RMW factor are positive and are estimated slightly more accurately than other statistically not significant factors; this suggests that Bitcoin returns comove more with high profit rather than low-profit firms. The point estimates on the MOM and CMA factors are very inaccurate.

The common stock factor exposures of the Ripple returns and compares them to the Bitcoin returns for the same time. The Bitcoin returns for this time have similar risk exposures as those in the full sample but have smaller and mostly insignificant alphas. We now turn to the analysis of Ripple. The alphas for all of the considered models are statistically significant. The unconditional alpha of the period is 38.15 per cent per month and is more than twice as large as that for Bitcoin.

The CAPM adjusted alpha is about the same as the unadjusted alpha. The CAPM beta is about half the size of Bitcoin and is not significant. In contrast to Bitcoin, there are statistically significant large negative loadings on the HML factor within the 5-factor and 6-factor models. The exposures to the other factors are not statistically significant. In summary, Ripple has performed better than Bitcoin for the corresponding time, and its returns comove with growth rather than value firms.

B. How to Handle Price Volatility

Given the fact that cryptocurrency is highly volatile, it does not mean that one cannot make money out of it. A patient and attentive investor can always make money out of the crypto trade. To start with one should not invest more than 5% of his investible surplus in cryptocurrencies and always research any cryptocurrency you invest. Track its price movement for few days and try to assess the downside risk before making any trade. Bitcoin volatility is also driven, to an extent, by these investors. It is unclear how Bitcoin whales – investors with BTC holdings in the tens of millions or more – would liquidate their significant positions into fiat currency without affecting Bitcoin market price. If the whales were to begin selling their bitcoin holdings suddenly, prices would plummet as other investors panicked as well.

C. Thefts and Scams

The biggest security concern for many people who invest in cryptocurrencies is the risk of hacking and fraud. Crypto scams have become common these days. According to reports, scammers impersonating Elon Musk had stolen over Rs 14.63 crore in digital currencies since October 2020. Also, crpto-crimes involve scammers requesting payment in cryptocurrency, or sending unsolicited offers to help you make money or increase your holdings. So it is necessary to avoid unsolicited offers related to crypto and buy your coins yourself using a reputable crypto exchange. Scammers often utilize dating websites to make unsuspecting targets believe that they are in real relationship. When trust has been granted, conversations often turn to lucrative cryptocurrency opportunities and the eventual transfer of either coins or account authentication credentials. Approximately 20% of the money reported lost in these scams.

D. Stay Invested for Long Term

If you are planning to invest in crypto for short term gains then chances are high that you may lose money in the trade. There have been many instances when cryptocurrencies have fallen for more than 20% in a single day. But if you stay invested for long term and continue to buy the digital currency on every big fall (of more than 20%), then you will make money in the longer term. It has been observed in the past these currencies rebound faster compared to any other assets class from a slump. Those who had invested in cryptocurrencies for at least three years and are still holding that investment are sitting on massive profit.

V. CHALLENGES AND PROBLEMS WITH CRYPTOCURRENCY

Though cryptocurrencies don't have any physical value, they hold a value which cannot be entirely determined. The cryptocurrencies erase the existence of third parties in each transaction and provide ownership of personal data for the owners. Aside from the following facts, these digital transactions of cryptocurrencies come with various challenges and problems.

The value of bitcoins has a self-determined value of all the supply and demand that they create [39]. The value of the bitcoins is directly proportional to their supply and demand; hence it can be said that the value of bitcoins is very unstable and unpredictable due to the variability in their supply [40]. However, since the year 2018, there has been a rapid increase of 30% in the economy in the industry as quoted by the Executive Director of the Indonesian Blockchain Association (ABI), Muhammad Deivito Dunggio. Devito or called Oham stated that the companies have started to compete for data, but this data is insecure and can be stolen even with complete security [40].

A. Mt. Gox Bankruptcy

A bitcoin exchange in Tokyo, known as Mt. Gox, was developed in 2010 to help users make transactions and exchange bitcoin with regular currency [41]. Mt. Gox suffered a security breach which led to a drop of 1% in the bitcoins price, although the price was soon stabilized and restored, many bitcoins were lost to this [41]. In 2011, they mistakenly sent over 2,500 bitcoins to invalid addresses which exposed many vulnerabilities in their protocols [41]. Although in 2013 they handled approx. 70% of the transactions, they had to declare bankruptcy after 850,000 Bitcoins were stolen from their customer and the company itself in a second hack [41].

B. The DAO Attack

Ethereum is the network on which value tokens ether are exchanged, they are the second most popular cryptocurrency. Ethereum has a Decentralised Autonomous Organisation (DAO). the job of the DAO is to structure the rules and decision-making apparatus of an organisation, this will eliminate the need for documents and people in governing to create a decentralised approach [42]. The DOA was the largest crowdfunding in history which had raised over $150m from over 11,000 members.

On June 17, 2016, the DAO was subject to attack when an attacker had started draining the DAO of ether collected from the sale of its tokens. On June 18 the attacker had managed to drain a large sum of over 3.6m ether into a *'child DAO'* which had the same structure as the DAO [42]- around a third of the 11.5m ether that had been committed to the DAO [43]. The value of ether had dropped by over $7. The DAO was eventually closed, the remaining funds were hard forked to move them to a recovery address for the original owners to convert them to Ethereum again. It was concluded that the DAO attack had happened due to the vulnerabilities in its codebase [44].

C. Alternative Cryptocurrency

There have been many other findings of cryptocurrencies which have failed in the past. There are many reasons why they couldn't survive; either they weren't sustainable enough or didn't give the expected results in terms of value and impact on the market. Some of these cryptocurrencies are BBQ Coin and Solidcoin [45], the others resulted in Sybil attacks or loss in their value in huge percentages [46].

VI. CONCLUSION

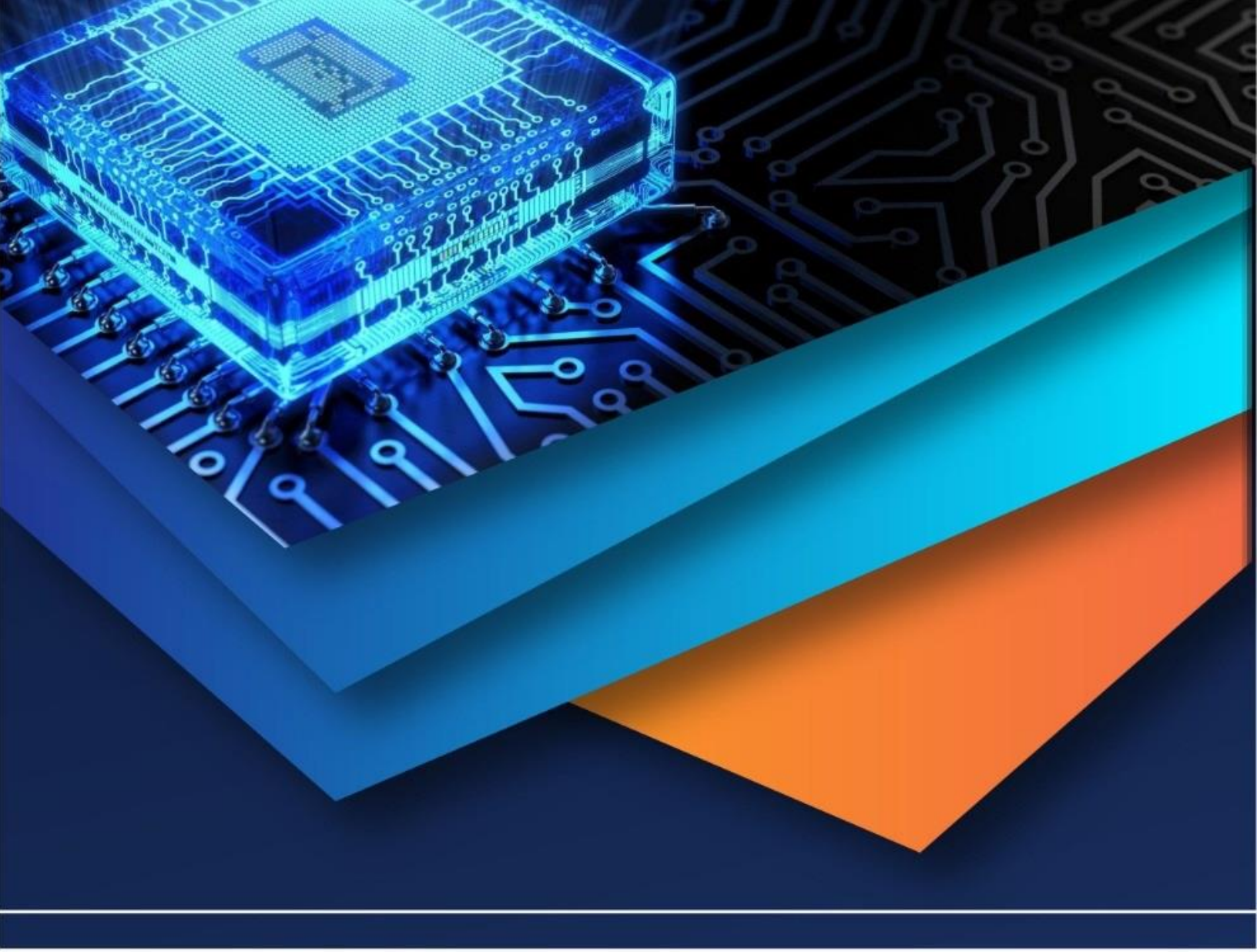
With the emergence of cryptocurrencies in the banking system, the banking systems have started to look more fragile in terms of accessibility and efficiency. Cryptocurrencies require minimal human interaction which makes them more accessible than banks. On the other hand, unlike the banks, cryptocurrencies are decentralized systems and work on peer-to-peer (P2P) technology over which the government has no control. This makes the government lose its power to decide, modulate, control and adjust the economic situation of the entire nation.

Cryptocurrencies, still have some drawbacks too! They lack the legal status of a currency that can be seen as a medium of exchange for commodities. Also, due to its limited supply, the cryptocurrency reserves are more likely to get exhausted if a huge population of miners grow. The mining process also requires a large amount of memory and the latest technology to validate transactions and consequently, generate new currency. It is a more secure and reliable system since it is hard to manipulate (due to the use of anonymous ID numbers in the transactions). At present, not all countries have been able to adopt the system of cryptocurrencies however, there still exist many banking systems that support and promote the use of digital currency.

REFERENCES

[1] Double spending. https://en.bitcoin.it/wiki/ Double-spending.
[2] anonymous. Proof of work. https://en.bitcoin.it/wiki/ Proof of work, 2014.
[3] Sunny King and Scott Nadal. Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. self-published paper, August 19, 2012.
[4] Andrew Miller, Ari Juels, Elaine Shi, Bryan Parno, and Jonathan Katz. Permacoin: Repurposing bitcoin work for data preservation. In Security and Privacy (SP), 2014 IEEE Symposium on, pages 475–490. IEEE, 2014.
[5] anonymous. Mining. https://en.bitcoin.it/wiki/Mining, 2014.
[6] Adam Back. The hashcash proof-of-work function. Draft-Hashcash-back-00, Internet-Draft Created,(Jun. 2003), 2003.
[7] anonymous. Mining difficulty metric. https://en.bitcoin. it/wiki/Mining#The Difficulty Metric, 2014.
[8] Karl J O'Dwyer and David Malone. Bitcoin mining and its energy footprint. In Irish Signals & Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communications Technologies (ISSC 2014/CIICT 2014). 25th IET pages 280– 285. IET, 2013.
[9] Colin Percival and Simon Josefsson. The scrypt password-based key derivation function. available at ietf.org, 2015.
[10] anonymous. Sha2 and scrypt. https://www.coinpursuit.com/pages/ bitcoin-altcoin-SHA-256-scrypt-mining-algorithms/, 2014.

[11] anonymous. Proof of stake. https://en.bitcoin.it/wiki/ Proof of Stake, 2014
[12] Gavin Wood. Ethereum: A secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper, 2014
[13] anonymous. Ethash. https://github.com/ethereum/wiki/ wiki/Ethash, 2014.
[14] David Schwartz, Noah Youngs, and Arthur Britto. The ripple protocol consensus algorithm. Ripple Labs Inc White Paper, page 5, 2014
[15] Harry Kalodner, Miles Carlsten, Paul Ellenbogen, Joseph Bonneau, and Arvind Narayanan. An empirical study of namecoin and lessons for decentralized namespace design. Technical report, Citeseer, 2015.
[16] Evan Duffield and Kyle Hagan. Darkcoin: Peertopeer cryptocurrency with anonymous blockchain transactions and an improved proof of work system. available at bitpaper.info, 2014.
[17] Daniel J Bernstein. Chacha, a variant of salsa20. In Workshop Record of SASC, volume 8, 2008.
[18] https://www.fortunebusinessinsights.com/industry-reports/cryptocurrency-market-100149
[19] Raymaekers, "Cryptocurrency Bitcoin: distribution, challenges and opportunities," Journal of Payments Strategy & Systems, vol. 9, no. 1, pp. 30-40, Spring 2015.
[20] Gabi Stern. (2015, April) Bit post. [Online]. http://bit-post.com/players/bitcoin-regulation-around-the-world-the-current-state-5627
[21] Virtual Currency Today, "Regulation of Virtual Currencies: A Global Overview," Virtual Currency Today, 2015.
[22] https://www.weforum.org/agenda/2022/03/where-is-cryptocurrency-regulation-heading/
[23] (2015, April) Coin Center. [Online]. https://coincenter.org/survey
[24] Blockchain info. [Online]. https://blockchain.info/
[25] Virtual Currency Today, "Virtual Currency 101 for Retailers," Virtual Currency Today, 2015
[26] Li X. The technology and economic determinants of cryptocurrency exchange rates: The case of the Bitcoin. Decision Support Systems. 2017;95:49-60
[27] Harwick C. Cryptocurrency and the problem of intermediation. The Independent Review. 2016;20(4):569-588
[28] Briere M, Oosterlink K, Szafarz A. Virtual currency, tangible return: Portfolio diversification with Bitcoin. Journal of Asset Management. 2015;16(6):365-373
[29] Cryptocurrency Returns | IntechOpen
[30] Fama, E. F., and K. R. French. 1993. Common risk factors in the returns on stocks and bonds. Journal of Financial Economics 33:3–56.
[31] Satoshi Nakamoto. (2008) Bitcoin: A Peer-to-Peer Electronic Cash System. [Online]. https://bitcoin.org/bitcoin.pdf
[32] Scott Nadal Sunny King. (2012, August) PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake. [Online]. http://www.peercoin.net/assets/paper/peercoin-paper.pdf
[33] Larry Ren, "Proof of Stake Velocity: Building the Social Currency of the Digital Age," 2014
[34] https://ideas.repec.org/p/red/sed019/160.html
[35] https://www.timesnownews.com/cryptonow/article/risk-vs-return-is-it...
[36] https://www.researchgate.net/publication/355068315_Analysis_of_Return...
[37] https://voxeu.org/article/risks-and-returns-cryptocurrencies
[38] https://www.sciencedirect.com/science/article/pii/S0275531920309557
[39] Swito, A. Michalczuk, and H. Josi, “Quaternion Watershed Transform,” vol. 1, no. 1, pp. 567–578, 2019, doi: 10.1007/978-3-030-14802-7
[40] A. Denni, van E. Patrick, B. Marat, and L. Andrea, “Do consumers really trust cryptocurrencies?,” Marketing Intelligence & Planning, vol. ahead-of-p, no. ahead-of-print. Jan. 01, 2020, doi: 10.1108/MIP-01-2020-0036
[41] Mark Karpeles. Clarification of mt. gox compromised accounts and major bitcoin sell-off, 2011.
[42] https://www.coindesk.com/learn/2016/06/25/understanding-the-dao-attack/
[43] https://en.wikipedia.org/wiki/The_DAO_(organization)#:~:text=On%20June%2017%2C%202016%2C%20the,time%20at%20around%20%2450M.
[44] https://www.gemini.com/cryptopedia/the-dao-hack-makerdao
[45] David Kuo Chuen LEE. The cryptocurrency revolution and its impact. Self-published, 2014.
[46] William J Luther. Cryptocurrencies, network effects, and switching costs. Contemporary Economic Policy, 2015.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY