John Creger

CS 463 Spring 2024

UIN 01154971

# Cryptocurrency

Cryptocurrency, once an emerging technology seemingly on the fringe of the information technology and financial world, is here to stay and now has major implications across various industries including information technology and financial markets. Digital currencies, blockchain, digital tokens, and NFT's to name a few that are rising to fame on to the markets and making a splash. These new technologies are confusing, to say the least, and navigating their intricacies requires an in-depth analysis. This paper will explore the basics of cryptocurrencies as well as the history, key figures behind some of the more prominent coins, and a few speculative futures, envisioned by the founders and current advocates of cryptocurrencies.

The term cryptocurrency is a general term used to describe an entire marketplace and cryptographical framework that has been created by some of the leading mathematicians and cryptographers around the world. The original term "cryptocurrency" entered the public domain in late aughts with the rise of Bitcoin [1]. Cryptocurrencies can be best described as a digital cryptographical system for the distribution of tokens. These tokens are then used as a medium of peer-to-peer exchange and are accounted for on a centralized ledger [1]. The cryptocurrency marketplace has exploded in recent years and there are thousands of systems that issue tokens. A few prominent cryptocurrencies include Bitcoin, Ethereum, Cardona, XRP and Solana. As Bitcoin was the original, other cryptocurrencies based on similar cryptographic schemes are often referred to as Altcoins [1]. Cryptocurrency has many names and is often used interchangeably with similar terms.

Cryptocurrency has had many prominent figures, some good and some bad, since the introduction of Bitcoin in 2009. Sometimes regarded as the founding father of cryptocurrency and creator of Bitcoin, is a shadowy figure known only as Satoshi Nakamoto [2]. This is a pseudonym as his identity is still not known. Vitalik Buterin is the founder of the Ethereum currency, the second largest digital currency. His influence was significant as he saw some of the shortcomings with Bitcoin and wrote the Ethereum code open sourced allowing the public to potentially improve it and then develop their own currencies. Not all figures in the crypto area are positive. Sam Bankman-Fried founded the crypto exchange FTX [2]. Through fraudulent business dealing and conspiracy, FTX collapsed, and a lot of people lost a lot of money. SBF was imprisoned and ordered to pay billions in fines [2]. These types of stories lead people to not trust cryptocurrency as they see it as an outlet for illegal activity and money laundering [2]. For example, the case of the Silk Road, a dark web website dedicated to the sale of illegal goods and services. The cryptocurrency arena is filled with innovators, entrepreneurs and visionaries hoping to enhance the world with crypto.

Cryptocurrencies rely on a decentralized ledger to maintain integrity and security. This ledger is based on blockchain technology. The blockchain is a public ledger of all transactions that have ever been implemented within the cryptosystem [3]. Blockchains can be used outside of cryptosystems as they can play a pivotal role in real estate transactions The chain consists of chronologically completed blocks of transactional data based on the previous blocks. A block is a data structure containing transaction data and includes five parts, the magic number, the block size, block header, a transaction counter and the actual transaction [3]. Every time a transaction takes place within the cryptosystem a block is created from the previous block using hash functions, which is stored in the block header. These hash functions are a one-way function that uses the data from the previous block to compute a new output. This process ensures that the data cannot altered without effecting the entire blockchain [3]. The blockchain is therefore comprised of many individual blocks that complete the cryptosystem ledger and is the backbone to any cryptosystem.

Blocks are added to the blockchain once they are verified through a process called mining. As an example, when a transaction happens in the cryptosystem, in which a payer sends some currency to a payee, the miner checks this transaction to make sure that the people involved are real and the payment is not a duplicate [3]. The first block in a crypto currency system is known as the genesis block. The genesis block contains the first transaction on the chain contains the first hash, thereby laying the foundation for the entire chain and establishing a traceable chronological path [3]. This mining process takes considerable resources to compute and is often time consuming. These transactions are validated in one of three ways, proof of work, proof of stake, or proof of retrievability. Once the transaction is validated by the miner, the block is added to the blockchain, and the miner is rewarded for the effort and is given a fraction of the newly introduced coins unlocked from the mining process [3]. Another key component for the success of the blockchain is the nonce. A nonce is the random number miners attempt to calculate to complete the validation of the block. Finding the nonce is the portion of the of mining that is the most resource intensive and therefore takes the most time and uses the most power [3]. These blocks are added to the distributed servers to ensure that they are public and therefore seen by the entire community. Being public is an added measure to ensure the continued validity of the entire blockchain. Maintaining the blockchain is the responsibility of the community of miners and users who stake their coins.

A noteworthy event that occurs in cryptocurrency system is known as a halving. These events are scheduled into the crypto protocol at predetermined times and reduce the amount of currency obtained by a miner who successfully completes a block by half the existing value [4] For example, for every 210,000 blocks, Bitcoin will conduct a halving event [4]. The primary purpose of crypto halving events is to manage the inflation rate of a cryptocurrency and ensure its scarcity, a key factor in crypto systems [4]. Reducing the rate at which new coins are introduced into circulation, halving events help maintain a predictable and diminishing supply of the cryptocurrency [4]. There is a total of 21 million bitcoin available for mining. This is a fixed number and will never be increased, although it is worth noting that bitcoin can be broken into smaller and smaller pieces giving a huge supply of usable currency. At its current rate bitcoin won't be completely mined for another 116 years or in 2140 [4]. These halving events are often highly anticipated, media driven and often create bull markets in the cryptosystem. These bull

markets lead to increased demand from investors seeking to capitalize on potential price appreciation. This demand-supply dynamic can contribute to price volatility in the lead-up to and aftermath of a halving event. As in the case right now, Bitcoin is scheduled for a halving event in 2024 and the price of bitcoin is up 44.62% year to date according to MSN.com. By reducing the rate of new coin issuance and increasing scarcity over time, halving events play a critical role in maintaining the economics of a crypto cryptocurrency.

The biggest limiting factor of scalability is maximum throughput and latency. The scalability of blockchains has been recently exposed with the popularity of cryptocurrencies. There have been numerous studies on blockchain and cryptocurrencies which has led to the perceived blockchain trilemma [5]. The three important properties of a blockchain system must include decentralization, security and scalability. The trilemma points out that these three conditions cannot happen at the same time, as an increase in one property would negatively affect one or two of the others [5]. Chains can be as long as you want in theory, but latency and quality of experience is going to hinder development past a certain point. According to Kyle Croman, the maximum throughput for Bitcoin is 7 transactions per second (TPS), while VISA can accommodate nearly 4000 TPS [5]. This drastic difference in throughput will ultimately hinder Bitcoin and other similar cryptocurrencies from reaching their potential market capitalization.

The blockchain works because it is a peer-to-peer distributed ledger technology or DLT, that keeps track, chronologically, of all transactions within the system. This ledger is not centrally stored and therefore stored on many nodes around the world. These nodes all maintain an identical copy and are updated simultaneously [6]. Each one of the nodes across the network is responsible for ensuring the ledger runs a consensus algorithm which confirms the accurate version of the ledger is stored on the node [6]. Consistency is critical to the functionality trustworthiness of the blockchain because if different versions of the chain were to exist, we would not know who had the current or correct version.

Blockchain technology is commonly used associated with the use of cryptocurrencies. However, many applications and sectors of the economy are set to benefit from the technology. The applications of blockchain can be divided into two types: Financial and Non-Financial applications [7]. An example of a non-crypto financial application would be securities issuance, trading, and settlement. A company would go public and offer shares, similar to an IPO, but they wouldn't have to use a bank or third party intermediatory [7]. Smart devices could use blockchain to store their communication with much higher-level security within the internet of things (IoT) [7]. Additionally, Smart contracts are currently being implemented within block chain technology. Smart contracts are digital contracts that are performed automatically within the block chain when certain requirements are met [7]. The contracts allow for the instantaneous execution of agreements between all parties without a middleman, leading to lower costs and increased efficiency [7]. The applications of blockchain technology are only beginning to reach their full potential and will revolutionize many aspects of online commerce and communication.

Cryptocurrencies have gained popularity for a variety of reasons, one being the security they provide. The decentralized ledger of the blockchain ensures that a single point of failure

could not exist and therefore the chain will not be deleted. The underlying infrastructure of the blockchain and crypto currency is where their security lies. For example, as mentioned above miners use proof of work, stake or retrievability to validate the blocks prior to adding them to chains[3]. This work ensures that forks don't occur and all participants in the transactions are authenticated and real [2]. The Block chain is tamper-proof based on the hash functions employed within them. The hash function is based on the hash of the previous block, therefore a change in one block would cause ripple effort and change all validated blocks after the altered block, which would be invalidated by all the nodes working on the blockchain [3]. A known vulnerability to the blockchain and cryptocurrency is the 51% attack [1]. This attack is based on the theoretical chance that a single entity was able to control over half of the nodes in the crypto system. If that were the case, that single entity would be able to change the chain at will because they would be able to approve the changes to the chain as a majority with other nodes not having a say [1]. This type of attack, although technically feasible, is highly unlikely due to the shear quantity of resources required and the potential financial gain is like outweighed by the resources required [1]. Cryptocurrencies are secure based on the cryptography of the blockchain technological properties.

An emerging protocol that blockchains are being built on is proof of human work (PoH). This type of proof requires that an actual human has done a moderate amount of work to solve a puzzle or challenge to validate a crypto transaction [8]. The key aspect of PoH is that the puzzle needs to be moderately hard for a human to solve, easily computer generated, but very hard for a computer to solve, including the computer that created the puzzle [8]. HumanCoin is the first crypto system that uses PoH and therefore has human miners. Human miners are touted as a big advantage for many reasons and why they have grown in popularity. This method is more ecofriendly, as traditional crypto mining is done by resource heavy computers and requires significantly more power [8]. These puzzles could also be educational, fun and even benefit society as whole [8]. An early example of these puzzles is CAPCHTA or Completely Automated Public Turing test to Tell Computers and Humans Apart. These tests include distorted text that a human could easily decipher, or a series of real photographs and the user must choose all the photos with a streetlight in the photo [8]. These tests are very difficult for a computer to understand therefore they are an excellent tool to prevent bots from entering certain areas of the internet. These tools are still in their infancy and one day be the foundation of the PoH protocol in cryptocurrency systems.

The Cryptographic techniques that cryptocurrencies employes are the same functions that we have learned about over the last 12 weeks. I think the most prominent is the hash functions. We learned about the SHA-1, SHA-2 hash functions and how they worked to one way encrypt data. The backbone of the blockchain requires the use of a hash, whether its SHA1, SHA-256 or even MD5. This one-way function ensures the data integrity of the rest of the chain and provides security to the entire system. Cryptocurrencies also use asymmetric cryptography like RSA, with the use of public and private keys. Recently, AES or Advanced Encryption System has been used alongside blockchain to enhance the security of mobile text messaging [8]. AES is a symmetric encryption system taught in the first half of the semester and is the more secure continuation of DES. Another topic that we spent a significant number of resources on this semester was Elliptic Curve Cryptography (ECC). ECC is a prominent function in the Bitcoin cryptosystem as it uses

the elliptic curve digital signature algorithm to sign all transactions [8]. Cryptocurrencies employ many of the crypto schemes discussed throughout this course.

Cryptocurrencies provide several advantages over traditional fiat currency. A fiat current is centrally organized, government issued currency not back by any physical commodity. An example of a fiat currency is the US Dollar. Cryptocurrency can provide protection against inflation [10]. When governments print more money, they add money to the already circulating supply, ultimately devaluing the currency. Cryptocurrencies have a hard cap on their supply, therefore limiting the number of coins that can be mined [10]. Transparency is another major advantage of cryptocurrencies. The decentralization of the blockchain ledger allows for public scrutiny of all transactions that take place, preventing unlawful or corrupt transactions from occurring. Another advantage is the security offered by the high level of cryptography associated with cryptocurrencies and the blockchain. The speed at which cryptocurrency transactions take place is currently relatively slow. However new crypto systems are being built that will far surpass the transaction speeds of the typical credit and wire transfers [10]. Typical VISA transaction speed is nearing 4000 transactions per second (TPS), compared to Bitcoin at 7 transactions per second [5]. Newer crypto systems such as Solana can accommodate up to 65000 TPS, greatly surpassing the TPS of credit cards [10]. Cryptocurrencies have many advantages over the physical, fiat currencies that currently dominate the marketplace.

With all the potential positive attributes, not everything is perfect with cryptocurrency. There are few major disadvantages with need to hurtle before cryptocurrency becomes mainstream. With the green new deal that many politicians are pushing, crypto mining needs to find a more ecofriendly solution. Efforts are underway to address these concerns, with some cryptocurrencies exploring alternative consensus mechanisms that are more energy-efficient, such as Proof of Human Work, addressed later in the report [11]. Initiatives to transition to renewable energy sources such as wind and solar for mining operations are gaining traction within the cryptocurrency community [11]. Another disadvantage is the current volatility. Most cryptocurrencies are trading on speculation and therefore the value of these currencies can change by thousands of dollars in just a few days, even hours [10]. This volatility can make people very wealthy but also lose a significant portion of their investment if not will hopefully reside if cryptocurrencies become more widely used and as accepted a legitimate currency. Once you complete a transaction with cryptocurrency it is nearly impossible to get your currency back unless it is given back by the recipient [10]. The lack of oversite from regulators provides virtually zero consumer protection against fraud and other digital scams.

The future seems bright in the world of cryptocurrencies. Although it is obviously impossible to predict the future of anything, cryptocurrencies will probably play an ever-increasing role in our financial systems. Many will argue that much our current monetary system is essentially a digital currency, in the evidence that cashless payments far exceed the percentage of cash payments [12]. The development of decentralized finance (DeFi) applications built on blockchain technology like Ethereum, and other altcoins has the potential to disrupt traditional financial institutions such as big banks and insurance companies, offering decentralized alternative solutions for many financial transactions like lending, borrowing and wealth management [12]. Machine learning and Artificial Intelligence will soon play a key role in

cryptocurrency systems and the blockchain. Machine learning algorithms are currently able to solve the CAPTCHA problems mentioned earlier in the report and will further enhance crypto security and efficiency [8]. As blockchain technology continues to mature and develop, cryptocurrencies will most likely play an increasingly significant role in changing traditional financial systems, enabling greater transparency, and efficiency.

Cryptocurrency is an exciting new form of currency that has great potential for use across a multitude of markets. I think as more people come to fully understand technology, it will become more embraced and widely accepted. The cryptocurrencies and connected markets are right now, very volatile and the potential to lose lots of money is very real. The bigger technology associated with cryptocurrency is the blockchain. This new method of decentralized ledgers has uses across many fields and will undoubtedly revolutionize aspects of current professions. I think the advantages of anonymity and decentralization outweigh the potential dangers of the perceived illicit activity surrounding cryptocurrencies. I personally look forward to a time when centralized banks and governments have less control over the financial systems.

References


[1] I. G. Pernice and B. Scott, “Cryptocurrency,” *Internet Policy Review*, vol. 10, no. 2, May 2021. doi:10.14763/2021.2.1561

[2] “Sam Bankman-Fried,” Forbes, https://www.forbes.com/profile/sam-bankman-fried/?sh=89abcdf44490 (accessed Apr. 14, 2024).

[3] U. Mukhopadhyay *et al.*, “A brief survey of cryptocurrency systems,” *2016 14th Annual Conference on Privacy, Security and Trust (PST)*, Dec. 2016. doi:10.1109/pst.2016.7906988

[4] A. Meynkhard, “Fair market value of bitcoin: Halving effect,” *Investment Management and Financial Innovations*, vol. 16, no. 4, pp. 72–85, Nov. 2019. doi:10.21511/imfi.16(4).2019.07

[5] Q. Zhou, H. Huang, Z. Zheng, and J. Bian, “Solutions to scalability of Blockchain: A survey,” *IEEE Access*, vol. 8, pp. 16440–16455, 2020. doi:10.1109/access.2020.2967218

[6] N. Barney, S. Troy, and M. K. Pratt, “What is distributed Ledger Technology (DLT)?: Definition from TechTarget,” CIO, https://www.techtarget.com/searchcio/definition/distributed-ledger (accessed Apr. 14, 2024).

[7] M. Nofer, P. Gomber, O. Hinz, and D. Schiereck, “Blockchain,” *Business & Information Systems Engineering*, vol. 59, no. 3, pp. 183–187, Mar. 2017. doi:10.1007/s12599-017-0467-3

[8] J. Blocki and H.-S. Zhou, “Designing proof of human-work puzzles for cryptocurrency and beyond,” *Theory of Cryptography*, pp. 517–546, 2016. doi:10.1007/978-3-662-53644-5_20

[9] M. Mujeerulla, Preethi, Md. S. Khan, and D. S. Sakkari, “Demerits of elliptic curve cryptosystem with bitcoin curves using Lenstra–lenstra–lovasz (LLL) lattice basis reduction,” *Arabian Journal for Science and Engineering*, vol. 49, no. 3, pp. 4109–4124, Sep. 2023. doi:10.1007/s13369-023-08116-w

[10] N. Tambe, “Advantages and disadvantages of cryptocurrency in 2024,” Forbes, https://www.forbes.com/advisor/in/investing/cryptocurrency/advantages-of-cryptocurrency/ (accessed Apr. 14, 2024).

[11] F. Mustafa, S. Lodh, M. Nandy, and V. Kumar, “Coupling of cryptocurrency trading with the Sustainable Environmental Goals: Is it on the cards?,” *Business Strategy and the Environment*, vol. 31, no. 3, pp. 1152–1168, Nov. 2021. doi:10.1002/bse.2947

[12] M. Ciarko, G. Poszwa, A. Paluch-Dybek, and M. Caner Timur, “Cryptocurrencies as the future of money: Theoretical aspects, blockchain technology and origins of Cryptocurrencies,” *Virtual Economics*, vol. 6, no. 3, pp. 70–93, Sep. 2023. doi:10.34021/ve.2023.06.03(5)

[13] “Visa crypto thought leadership – a deep dive on Solana,” Visa, https://usa.visa.com/solutions/crypto/deep-dive-on-solana.html (accessed Apr. 14, 2024).