Blockchain and Other Cryptographic Concepts and Their Application in Cryptocurrencies

Gregory S. Oehm

School of Cybersecurity, Old Dominion University

CS 463: Cryptography for Cybersecurity

Prof. Nasreen Arif

August 3, 2025

Introduction

Cryptocurrencies have, within the last decade, quickly emerged as an alternative to other forms of money. Bitcoin, Ethereum, and Dogecoin are among the most discussed of these currencies, but countless others have been created and traded widely, as well. Blockchain technology forms the basis of these cryptocurrencies, permitting trading to be validated and carried out reliably. Without blockchain technologies, which inherently make use of several cryptographic concepts, these types of currencies would very likely be impossible to use effectively. Cryptocurrencies, through providing a decentralized method of exchange separate from major organizations, such as banks or governments, offer some notable benefits over more traditional currencies. This same detachment from existing infrastructure, however, has also contributed to some of the limitations present on the use of cryptocurrency. Though cryptocurrencies hold great potential to replace or complement other currencies in a digital world, it seems unlikely that their use will become commonplace at any point in the near future.

Understanding Blockchain

The foundational technology behind cryptocurrencies is that of the blockchain. Consequently, it is crucial to understand how blockchains operate in order to fully appreciate how they are utilized by various types of cryptocurrencies. A blockchain is, at its core, a list that provides a method of sharing information among different users in a network, including the Internet, which further permits this information to be validated by multiple sources, thereby ensuring the integrity of each piece of data [1]. Each user with access to the blockchain which, in the case of cryptocurrency, can be essentially any person or system, is granted access to a list, which is the same list shared by all other users. The items that this list is composed of, as one might perhaps be able to infer from the name "blockchain," are single "blocks" of data. Each block is linked to the previous and subsequent blocks through the information carried within it, permitting its overall data to be free from alterations later on, after the block has been confirmed [1]. The exact data carried in each block might vary, depending on the context in which the blockchain is used. However, all applications of blockchains require some basic information to be contained within each block. Such information typically includes, at a minimum, the hash of the previous block, a timestamp of the point in which each block is created, and a random nonce value [2:184]. Each of these pieces of information must be present within each block for the blockchain as a whole to function properly, in nearly all implementations. A hash value of the previous block is needed to link each block together in sequence. This ensures that the data used in each individual block has an impact on all of the blocks that come after it in the chain, thereby connecting them [2:184]. A timestamp is also needed for each block. This provides clarity as to the order blocks should be placed within the blockchain [1]. Without a timestamp, it may be unclear as to which order to blocks should be added in, if they are confirmed at similar times. The nonce value in each block, which should not be repeated by any later blocks, adds additional uniqueness to each block, and thus the hash produced from it. Each of these pieces of information contribute to the integrity and immutability of each block. Without this data, it may be harder to detect when deceptive changes are made to certain blocks, or where that change has been made in the chain. Since the current block's hash is based on the previous block, which is itself based on each of the previous blocks and their hash values, even a minor change in a block can be easily identified, due to the fact that it would conflict with the hashes of every single block that follows it in the chain. None of this focus on the effective permanence of blocks in the blockchain would matter to any significant degree if anyone could add any block at any time, however. Consequently, another important aspect of blockchains in the way in which blocks are

able to be added to the chain. The process of block addition is not necessarily completed by a specific user or system on the network, but by the collective network as a whole, which agrees upon the block and its constituent components. The exact method in which the block is confirmed might differ between different blockchain implementations, but agreement must be achieved across a certain number of systems in the network, often a majority or a higher proportion of the total network [3]. At this point, the block has been validated, and can be added to the list accessible by all users [2:184]. There is typically no centralized server that adds the block into this shared list. Rather, the block is collectively agreed upon and added to the list by each system on the network, in a distributed fashion. Each system can compare its own list against others in the network. When a new block is created and successfully added to the blockchain, it is sent to all other nodes, or users [4:401]. As a result, consistency is maintained throughout each copy of the blockchain, with any missing blocks or anomalies in any individual copy of the blockchain being able to be rectified quickly. All aspects of the blockchain, including maintaining the existing list of blocks while adding new ones, are done collectively by each system, as opposed to being accomplished through a single server. Put together, the blockchains used in both cryptocurrencies, and other purposes, are composed of a series of connected blocks, each of which is, as a result of the way in which blocks are recorded and maintained, confirmed by most or all others on the network, and consequently remains largely permanent and unchangeable.

Scalability of Blockchains

The fact that the entirety of a blockchain depends on each block that came before it, back to the very first block in the chain, poses some notable concerns related to the scalability of these technologies or, rather, the lack thereof. While one can technically have extremely long blockchains, shared among each relevant system, some difficulties may arise if the shared list becomes too large in size. For one, if the length of the blockchain becomes too large, the amount of storage that must be allocated to it on each system could prompt it to become unusable [5]. Though there are methods to circumvent this, such as by not storing the whole blockchain on each device, this brings with it its own issues. To ensure that fraudulent changes are not made, and that each device can access previous blocks when they are required, at least some systems need to have the entirety of the blockchain stored, and there must be enough of these systems that all users can obtain the blocks necessary to verify current and past changes. In addition, as the blockchain becomes larger, the infrastructure that must be in place to support the timely communication of each block itself becomes greater, requiring substantive effort on the part of users [5]. To resolve this issue, one might suggest a single, central server to store and mediate the blockchain. Such a structure, however, returns the problem of centralization back into the equation, one of the very problems that blockchains seek to avoid. Since this kind of consolidation goes against one of the very purposes and benefits of blockchains, it is highly questionable whether it should be used. Scalability concerns about blockchains also stem from the need for greater levels of communication across the network. This may pose problems in the ability for each block to be proven accurate and added to the blockchain, given the increasing frequency of updates that must be made to the blockchain with a higher number of users. Since a consensus must be reached before a block can be added to the blockchain, there would potentially be a need for many devices to expend computational effort to confirm transactions. Even with Bitcoin's arguably niche market at the current time, verifying transactions can take upwards of ten minutes, an issue that might become more pronounced as more individuals make use of Bitcoin and thus add more blocks to the blockchain at a more rapid pace [5:107]. Should

Bitcoin or other cryptocurrencies become more heavily used at a global scale, these issues could seriously hinder their effectiveness, bogging down transactions and reducing overall productivity. These difficulties are prompted by the need for all users to be able to keep track of all transactions in a public manner, compounding the computations and communication that must be performed. The conflicting nature of decentralization and scalability poses a major challenge for cryptocurrencies like Bitcoin, and for all applications that seek to make use of blockchains at a wider scale.

Applications of Blockchain Technology

The applications of blockchain technologies are surprisingly numerous. Cryptocurrencies like Bitcoin are perhaps the most obvious example of blockchain being used in practice. There are, however, a multitude of other ways in which blockchains can be applied. One type of these implementations, which has become the subject of much attention in recent years, is non-fungible tokens, commonly referred to as NFTs. Much like cryptocurrencies, non-fungible tokens utilize publicly available blockchains to describe ownership of certain unique digital items. Like cryptocurrencies, these can be traded to different individuals through the addition of blocks to the blockchain, thereby signaling a change in ownership. Often, these tokens represent ownership over a piece of artwork or other intangible item, though they can be applied to other digital goods, as well. Though non-fungible tokens have been the source of much contention among the general public, who, with good cause, may see many implementations of NFTs as shallow attempts to gain wealth for their creators, the overall concept does hold promise. Future applications of non-fungible tokens, that make use of it in a beneficial way, may find great success. Applications that use blockchains do not necessarily need to be public, either. Blockchains can restrict access to a limited number of users, such as those in a particular organization or set of organizations. This might be done to keep track of physical items or records in a business or other organization where integrity and transparency are a primary focus [6]. Overall, blockchains have at least some use cases in any situation where a number of people or systems need to keep track of the transfer of some kind of item, without the ability or desire to have a central authority in place to do so.

Cryptocurrency as an Implementation of Blockchain

Blockchains form the foundation of cryptocurrency. Cryptocurrencies were first created in 2009 with the implementation of Bitcoin [4:399]. It was not until several years later, however, about the mid-2010s, that Bitcoin attained the popularity it holds today. At around that point, numerous other cryptocurrencies began to be created. Within the blockchains used by cryptocurrencies, individual blocks contain information that indicates ownership of different pieces of cryptocurrency, or a change in the ownership of cryptocurrencies. This allows individuals to exchange these items safely and securely.

Security of Cryptocurrencies

The security of cryptocurrencies comes from their use of blockchains, and the cryptographic concepts that they are underpinned by. Since copies of a block are stored on not just one computer, but potentially thousands or millions of systems, one can be assured that the whole is unlikely to experience major disruptions. Its use of hashes, too, provides strong protections against tampering. In order to modify any previous block one would, by extension, also need to modify the hash values of each block that follows, a clearly infeasible task [1]. The fact that each additional block added to the blockchain must be confirmed by many other systems on the network, too, provides significant protection against fraudulent additions. The nonce used in each block also helps to distinguish one block from another. These aspects

prevent, for example, someone from altering a block on their own system in order to trick others into thinking that a previously spent bitcoin is still in the possession of the individual. Such a change would be easily identified by the many other systems that have unmodified blocks.

Cryptocurrency Mining and Puzzle Solving

The underlying assumption of blockchains, and thus cryptocurrencies, is that there will be systems willing to perform the computational effort needed to verify and confirm additions to the blockchain. There is a significant amount of mathematics that must be performed and completed in order to confirm or deny the validity of transactions and add them to the blockchain. Some cryptocurrencies ensure that this is the case by linking these computations to the distribution of cryptocurrencies, as is the case with Bitcoin. In Bitcoin's proof-of-work system, those that perform these calculations alter the nonce value of the block until the hash value is deemed to be appropriate, based on predefined requirements [7]. At this point, the block and the transactions within it can be appended to the blockchain. If this were not done, it would be relatively easy for a malicious individual to make alterations to blocks. Put simply, sets of transactions are added to the blockchain by solving puzzles, in a sense. Those that "mine" cryptocurrency, or perform the calculations needed to support the system overall, are potentially rewarded with ownership over new cryptocurrency if they are the first to find an acceptable nonce and subsequent hash, making the computational effort worthwhile, while allowing new cryptocurrency to enter into circulation, which it itself necessary [2:184]. Consequently, these kinds of puzzle solving contests permit cryptocurrencies like bitcoin to be continuously maintained without the need for a central authority to regulate them. It is for this reason that such methods are widely used across different kinds of cryptocurrencies.

Cryptographic Concepts Used in Cryptocurrencies

Several cryptographic techniques discussed within this course are utilized within various cryptocurrencies. Hashes, of course, form an integral part of currencies, in that it permits the blockchain to function at all. Through a specific hashing algorithm, such as a SHA hash function, a distinctive short string is generated from the contents of a particular block through several compression rounds. The entire concept of blockchains is somewhat akin to cipher block chaining, as well, in that the hash of one block is used in the creation of the next, though there are clearly some differences. Cryptocurrencies also make substantive use of public-key cryptography. In order to both send and receive cryptocurrency from other users, one must be able to reliably determine the identity of these individuals, without a predetermined shared secret. Public-key cryptography is well suited for this purpose. Each user possesses a public key and private key pair, which are inverses of each other, and the former is made public. The public key of others, then, is used to identify who should receive the cryptocurrency, while the private key is used to authenticate one's identity, such as through the use of a digital signature [1].

Advantages of Cryptocurrencies

Cryptocurrencies possess several notable advantages over other forms of currency, such as physical notes or coins, or other intangible forms of payment like bank-issued credit cards or debit cards. Perhaps the most clear of these advantages is that cryptocurrency is not bound by the material obstacles that might prevent traditional currency from being used. Bills or other physical money, of course, do little good when attempting to make purchases over the Internet. One cannot simply hand someone on the other side of the world paper money or coins, meaning that another method of exchange is needed. Digital currencies, like cryptocurrencies, can help to fulfill this need. Clearly, cryptocurrencies like Bitcoin are not bound by any physical location, and can thus be transferred to others who may be thousands of miles away. The lack of a central

authority also means that exchanges are not restrained by the will of banks or governments. Since transfers of cryptocurrency occur through the blockchain, there are generally fewer restrictions or fees imposed on the users of cryptocurrency. The fact that cryptocurrency is decentralized could be seen as an advantage in and of itself, as well. The users of cryptocurrencies, in many cases, would not be bound by the will of certain authorities, who may otherwise wish to exercise control over the transfer of funds. The protections and verification built into blockchain technology, too, also provide strong measures against counterfeiting. As the legitimacy of each transaction is confirmed by others, there is largely no way for cryptocurrency to be fraudulently created or used without being detected. While similar protections are also present in other forms of currency, their reliability is often weaker than that used by cryptocurrencies.

Disadvantages of Cryptocurrencies

Despite these potential benefits demonstrating that cryptocurrency can have real, practical applications, and providing promise for it to be a replacement or supplement to real currency in a digital space, cryptocurrencies in practice face many challenges that have, at the current moment, largely relegated them to being utilized as speculative investments by investors, as opposed to a true means of exchange. The most widely recognized function of cryptocurrencies, at least by the general public, is that of a speculative market. Many individuals may purchase cryptocurrencies with the expectation that their price will rise, potentially drastically, over time. Perhaps the most memorable instance of this relates to Bitcoin, the price of which has skyrocketed, with each Bitcoin now being valued at many thousands of dollars, far more than the pennies they were initially bought and sold for. Another unfortunate use is that of certain illegal endeavors. Though most cryptocurrencies can likely be tracked with some effort, due to the recorded nature of the blockchain and its decentralized focus, the belief that the transfer of cryptocurrencies is untraceable is still held by some. Consequently, cryptocurrencies like Bitcoin have not caught on, at least in respect to their intended use. Another factor prompting this is the fact that cryptocurrencies are generally not backed by a true authority, like a government or other powerful entity, evidenced by the vast number of cryptocurrencies that have been created in recent years. Some cryptocurrencies, often referred to as “memecoins,” are created solely as a way to make money, with no intention of actually being used as a true currency. Some individuals may seek to create these cryptocurrencies in order to take advantage of others, tricking people into thinking purchasing these cryptocurrencies is a smart investment, when this is most certainly not the case. This may encourage hesitancy to treat other, more legitimate cryptocurrencies as a true currency. Cryptocurrencies, due to their more technical nature, are also not very accessible to most people, favored only by the technologically inclined. Most individuals seemingly do not know how to obtain or utilize cryptocurrencies, with few going out of their way to educate the general public on its use. A key part of this is that cryptocurrencies are not distributed like a “real” currency, per se. Individuals instead obtain new cryptocurrency by mining, or solving the mathematical problems needed for the cryptocurrency to be reliably maintained through the use of programs [2:184]. Another important factor contributing to the limited use of cryptocurrencies is their polarized value, with cryptocurrencies either being worth too little to be used as a means of exchange in their own right, or too expensive to be accessible. This partially results from the fact that as the more popular a currency gets, the more it is worth, given that the quantity of cryptocurrency in circulation is limited. In situations where a cryptocurrency is sought after, like Bitcoin, individuals may be forced to pay for items in fractions of a cryptocurrency or, in the case of less popular currencies,

these same items may need to be paid for with hundreds or thousands of units of these cryptocurrencies. This is, of course, undesirable, bringing with it a whole host of technical and practical problems that most would wish to avoid. Even beyond the challenges these currencies pose by themselves, at the currency time, cryptocurrencies like Bitcoin have limited practical applications for most consumers, as few vendors accept cryptocurrency as a means of exchange. This is made worse by the volatility of these cryptocurrencies. Where "real" currencies are unlikely to experience major shifts in value within a short period of time, instead usually changing slowly over years or decades, the value of some cryptocurrencies can change quite drastically within a matter of days. Essentially, given that there is no true central authority regulating the use and distribution of cryptocurrencies, or backing it up with real-world value, combined with the fact that it does not already have widespread use, society as a whole is unlikely to adopt cryptocurrencies, as there is little motivation for individuals to do so. The fact that there are so many potential cryptocurrencies, too, has exacerbated this issue, with there potentially being no clear single candidate for which should be employed. The high number of cryptocurrencies available means that, while some hold more of a reputation than others, the validity of each is still questionable. There is also a strong argument to be made that the computational requirements cryptocurrencies possess has made them impractical for wide scale use. Even with their arguably uncommon use at the current time, cryptocurrencies might use up significant resources around the globe to maintain accuracy of blockchains, with many purchasing devices or computer components simply to perform the mathematical operations cryptocurrencies like Bitcoin require. This has also supplied threat actors with sufficient motivation to place malware on the computers of others for the express purpose of mining cryptocurrency. Additional users of cryptocurrencies would entail many more communications and operations to achieve a consensus in more frequent transactions. The need for each and every additional block to be confirmed in this way could be disastrous with a higher number of global users. The length of the blockchain would also potentially pose problems in accessing the relevant blocks, and in storing previous blocks on the blockchain. Many have pointed out that the existing diversion of computers and resources to support cryptocurrency is "wasting" energy, for a purpose that serves no practical effect, thus potentially having an adverse impact on the global climate, though the current impacts are arguably minor. Even so, at a larger scale, which would be the case if cryptocurrencies become widely used, these issues may become even more pronounced. Each of these characteristics, both those that are inherent to cryptocurrency and those that relate to external circumstances, pose roadblocks to the widespread use of cryptocurrency as a genuine tool for exchange. The computational effort needed to support a decentralized model, while spread out, is not insignificant. This, alongside other external considerations, might hinder a more wide scale use of cryptocurrencies like Bitcoin.

Conclusion

Cryptocurrencies have, relatively rapidly, become a part of the mainstream consciousness. Blockchain technology, and the cryptographic concepts that support it, are crucial to the existence of cryptocurrencies, providing much needed security in a decentralized fashion. While cryptocurrencies offer some notable advantages over traditional forms of currency, they are not perfect. Several key aspects of the way in which cryptocurrency operates, along with certain societal forces, have limited the potential for cryptocurrencies to be used in their intended manner. The adoption of cryptocurrencies is not simply a technical challenge, but a social, political, and economic one, as well. Personally, while cryptocurrencies seem interesting in theory, especially as a result of the way in which blockchain technology is used, I cannot see

them being used in the same way as traditional currencies. Though they could function as a sort of global currency separate from the control imposed by governments and other authorities, the surrounding challenges seem to make widespread adoption infeasible. Perhaps future developments will enable cryptocurrencies like Bitcoin or Ethereum to fulfill their intended purpose. At the current time, however, it seems unlikely that these currencies will become more widespread than traditional forms of currency, even in digital spaces.

References

[1] S. Susnjara and I. Smalley. “What is Blockchain?” Internet: https://www.ibm.com/think/topics/blockchain, [Aug. 2, 2025].

[2] M. Nofer, P. Gomber, O. Hinz, and D. Schiereck. (2017, Mar.). “Blockchain.” *Business & Information Systems Engineering.* [Online]. 59(3), pp. 183-187. Available: https://doi.org/10.1007/s12599-017-0467-3 [Aug. 2, 2025].

[3] J. Mansa. “What Are Consensus Mechanisms in Blockchain and Cryptocurrency?” Internet: https://www.investopedia.com/terms/c/consensus-mechanism-cryptocurrency.asp, Jun. 2, 2024 [Aug. 2, 2025].

[4] S. Barber, X. Boyen, E. Shi, and E. Uzun. “Bitter to Better — How to Make Bitcoin a Better Currency,” in *Financial Cryptography and Data Security*, 2012, pp. 399-414. [Online] Available: https://doi.org/10.1007/978-3-642-32946-3_29 [Aug. 2, 2025].

[5] K. Croman *et al*. “On Scaling Decentralized Blockchains,” in *Financial Cryptography and Data Security,* 2016, pp. 106-125. [Online] Available: https://doi.org/10.1007/978-3-662-53357-4_8 [Aug. 2, 2025].

[6] J. Abou Jaoude and R. George Saade. (2022, Jun.) “Blockchain Applications – Usage in Different Domains.” *IEEE Access*. 7, pp. 45360-45381. https://doi.org/10.1109/ACCESS.2019.2902501 [Aug. 2, 2025].

[7] A. Hayes, D. Clemon, and S. Kvilhaug. “Blockchain Facts: What Is It, How It Works, and How It Can Be Used” Internet: https://www.investopedia.com/terms/b/blockchain.asp, Mar. 24, 2025 [Aug. 2, 2025].