Old Dominion University

Cryptocurrency

How They Are Shaping the World Around Us

Clarence Virgil Kimbrell Jr

Cryptography CS 463

Professor Susan Zehra

November 30, 2022

Table of Contents

History of Currency

Throughout history, there have been many types of currencies have existed. Some estimates suggest it goes back nearly forty thousand years. It was designated as the upper paleolithic era during this time in human history. Archaeological studies found that hunters and gathers would trade flint items such as tools or equipment to each other. This is one of the first known uses of items as a currency between people. There were no markets to spend your flint items on like in our day in age. This connection between two people trading grew into something that our civilization could not live without. Fast forwarding thousands of years into the future in modern-day Turkey it is believed that the oldest form of currency that we use today was created. During the reign of King Alyattes, which was six hundred nineteen to five hundred and sixty B.C., the first considered minted coin was created. It was slightly different from the ones we see today but the concept and design are the same. These coins were not used for conventional means for a few hundred more years. They grew in popularity and in the same place as, modern-day Turkey, it is also believed that is where the first tine of permanent stores arose. The coins were exchanged for items and services that generated wealth for the first time outside of royalty and rulers. A few hundred years later, paper money was invented in modern-day China. This was created to ease the load of having to carry heavy quantities of metals everywhere you went to purchase things. However, the paper currency that was created in the Tang Dynasty was six hundred eighteen to nine hundred and seven C.E. This only lasted a few years because of conquest by a neighboring rival. Then fast forwarding a few more thousand years we have the oldest currency that is still in circulation today. The British pound shilling dates back nearly one thousand two hundred years. This was the high Middle Ages when borders were being established between regions for permanent kingdoms. They started the same way as the ones in Turkey which were coins. These are still used in a day in age where money is no longer physical. These are the origins of traditional money that we think of today and use with knowing little of the history behind their creation.

What are Cryptocurrencies?

Cryptocurrencies are older than most people believe them to be. The first use of the word cryptocurrency was in nineteen eighty-nine by a famous cryptographer named David Chaum. He has been credited with the invention of digital cash which was computed using cryptography to protect and confirm transactions. His contribution to society was extraordinary because what he created is used worldwide and has the potential to replace traditional money as we know it. He is still alive today and is referred to as “the godfather of cryptocurrency.” Many have said if it was not David Chaum, it would have been someone else later down the road. This is because of how involved we are as a society with the internet and things being digital. But what is cryptocurrency? According to the Merriam-Webster official dictionary, the definition of cryptocurrency is defined as “any form of currency that only exists digitally, that usually has no central issuing or regulating authority but instead uses a decentralized system to record transactions and manage the issuance of new units and relies on cryptography to prevent counterfeiting and fraudulent transactions.”. Since these exist digitally and are decentralized, they have become one of if not the fastest-growing types of currency in existence. They gain value by how involved the user of it. Since their growing popularity, the cost of popular cryptocurrencies is valued quite high with zero signs of slowing down or halting.

What are some examples of Cryptocurrencies?

When most people hear or think of cryptocurrencies they think of the most popular ones. This makes sense because those are the ones getting the most coverage. Since the rise of cryptocurrencies, they have been compared in price to precious rare earth metals. Some people believe the only type of cryptocurrency is Bitcoin which could have not been further from the truth. A twenty-twenty-two study conducted by stastista.com estimated that there are over ten thousand types of cryptocurrencies. Some more popular than others of course the sheer number of kinds is eye-watering, to say the least. If we compare that to their physical counterpart there are only one hundred and eighty that exist currently in circulation today. There are fifty-eight times the number of cryptocurrencies than physical real money. The most popular types of the ten thousand are Bitcoin, Ethereum, Litecoin, and Ripple. After the main few it is widely considered to call the rest altcoins to differentiate the difference between them. Bitcoin was one of the pioneers of cryptocurrencies and is the most popular and valued among them. It is said the true inventor of Bitcoin is still shrouded in mystery but is currently credited to Satoshi Nakamoto. Then the second most popular form of cryptocurrency is Ethereum. This was created a whole six years after Bitcoin was invented and overtook many spots to become the second most used type. Litecoin was created in two thousand and eleven so it is three years older than Ethereum. This is considered the third most used type of cryptocurrency despite being older than most. One of the favorable attributes of Litecoin is that it allows for faster payments than most and more frequent transactions. Then finally we have Ripple which is slightly different from most other types of cryptocurrencies. This is because it can be used to track different kinds of payments and it is not limited to just cryptocurrency. Then can have its benefits if you purchase items in different currencies.

What is a blockchain?

Blockchains are used very commonly in the world of cryptography. The definition of cryptography from the Merriam-Webster dictionary states that it is “the enciphering and deciphering of messages in a secret code or cipher.” This is important to understand because blockchains are some of the foundations of cryptography. The applications of cryptography are endless and used nearly in all things online, without many users’ awareness. Blockchains are constructed by two foundational elements which are hashing and cryptography. Hashing takes data as input and outputs a plaintext or ciphertext. Blockchains are a technique that protects payments or information from two or more places. These are incredibly beneficial to everyone who is connected to online services. It protects users from malicious hackers stealing information. Cryptocurrencies rely on blockchains to encrypt data between transactions so no money is lost in the process. If it is not blockchains specifically it is some variation of it to encrypt and decrypt information. The application of blockchains is not limited to cryptocurrency we see them on most websites and online purchases that do not involve currencies like Bitcoin and Ethereum. These are a necessity that needs to be incorporated into all aspects of online media, banking, transactions, and more.

What is in the block of a blockchain?

Blockchain can involve hundreds if not thousands of blocks that contain information. Each block in a blockchain includes a hash or ciphertext from the previous block as well as transaction date and timestamps. To visualize blockchains in their simplest form I like to compare them to railroad tracks. Despite them being less technologically sophisticated they can be comparable. This is because each plank of wood could represent a block in a blockchain, and when elevation is involved in a railroad track the previous plank of wood needs to be represented in the next. If not, this could have cataphoric gaps for information and safety in blockchains and railroads respectfully. Then the collaboration between all blocks creates the final product which is a blockchain. It is important to know that blockchains operate from many different computers or hardware, and can not be altered without changing the previous block. It would be incredibly inefficient to do so because you would have to start from square one and then work your way back. Blockchains became popular through the use of cryptocurrencies such as Bitcoin. Since industries realize how useful they are they were applied to other aspects of the digital world around us.

How are they linked?

If we take our example from the previous section and expand further upon it. We realize that there is nothing that holds the railroad tracks in place until the metal rails are put in place. This is similar to how blockchains are linked together. They use different techniques and mechanisms to allow the blockchain to operate and let information flow through it. With Bitcoin, for example, they reorganize transactions by separating them into blocks that contain a concrete number of payments. Then these blocks are linked to previous blocks depending on a time-related chain.

When are the blocks added?

According to a study done by onezero.medium.com in twenty sixteen, they found that it depends on what kind of blockchain we are looking at. With Bitcoin on the rise to the dominant spot of cryptocurrencies, we will look more into them. On a blockchain, it is estimated that a new block gets added about every 10 minutes. We need to remember that each block contains information from the previous one. So early blocks that were added twenty to sixty minutes ago have been processed. As stated above it is really difficult to change the information in a block without having to restart. So, once it has been processed it is said to be irreversible. As a blockchain grows it becomes more secure because of the newer blocks of information that update the existing.

Who adds the blocks ---centralized server or distributed servers?

So, we know when blocks are added and how they are linked but who adds them? In cryptocurrencies like Bitcoin, the miners are held accountable for adding a new block to the chain. Bitcoin miners have a lot of responsibility because they need to create and confirm the integrity of the information provided. This is important because integrity is one of the core principles of the CIA triad. Which contains Confidentiality, Integrity, and Accountability.

Bitcoin operates in a distributed or decentralized configuration, allowing users worldwide to operate at any given time.

Who maintains the blockchain?

Since we discovered that blockchains are decentralized we need to ask ourselves how is this safe. So, miners add new blocks from wherever they are computing these transactions and they are added about every ten minutes. This is held together and maintained with the use of cryptography and protocols. Cryptography computes the transaction being added to the blockchain and if there is anything incorrect it will reject the transaction entirely. The protocols and cryptography involved can not be changed by users of Bitcoin so this allows it to maintain its open nature.

Are these scalable? Can the chains be as long as you wish them to be?

Yes, blockchains can be valued for the number of blocks within them. So, does that mean chains can be as long as you wish? In theory yes, they can be infinite. There is no limit on how long blockchains have to stop. It was noted earlier that the more blocks that are added into a blockchain they become more secure. This relation between security and the number of blocks on a very large scale does not directly correlate. Adding one block does not increase the security by a huge proportion, this is not to downplay the significance but when blockchains are in the millions. Adding one block does not make it unbreakable.

What are the performance implications of having long chains?

Multiple factors need to be taken into account when asked about the performance implications of having long chains. Just as with anything technology-related, if there are larger things to compute it will take longer to do so. This is no stranger to enormous blockchains such as Bitcoin. Since it is estimated that one hundred and forty-four blocks are added every day, one year's worth of blocks takes a long time to compute. Then there is another factor such as network connectivity if a user has slower internet speeds their mining computational speed is reduced. Another is if transactions are larger than average it can hinder performance. Lastly one of the biggest factors that could impact performance on long chains is simply the hardware being used. If a system is using older hardware the speed at which it can compute drops significantly.

How is consistency maintained among copies of blockchains?

The consistency is maintained among copies of blockchains by a peer-to-peer network. A peer-to-peer network commonly referred to as P2P is defined as a network that is created when two or more computers are connected to share resources. Since there is no centralized computer or server to check for consistency the creators of Bitcoin developed a way to provide consistency. This is done by checking for things just as verification, durability, and integrity. These are found in the data storage system that operates to maintain copies of blockchains to keep them consistent.

Examples of applications where blockchain technologies are being used.

There are countless applications for blockchains to be used throughout the digital world we live in. One application that popularized blockchains is cryptocurrencies. There are many variations of blockchains but they carry the same principle. Blockchains used by different cryptocurrencies have slight differences but achieve the same goal of recording and adding information that cannot be altered. Blockchains can be found in capital markets because they provide operational improvements and combine an audit trail. Since blockchains can not be altered it has protected companies from money laundering schemes. This is a crucial aspect because it provides an extra layer to a more attacked part of the digital space. We see the use of blockchains in the healthcare industry because tampering with patient information has become a growing trend. Some devices are connected to the internet which can be a target for malicious individuals. Then we see the uses of blockchains in voting because they provide protection and accessibility. The applications of blockchains are endless and will continue to grow rapidly as more things are incorporated into the online space.

Are these cryptocurrencies secure? What gives them the properties of reliability, tamper-proof, and uniqueness?

There will never be one hundred percent maximum security on anything we create. This also applies to cryptocurrencies. The main ones like Bitcoin and Ethereum have made it nearly impossible but there is still the smallest chance of breaches. As discussed earlier when more blocks are added to a blockchain it makes them more secure. So, if the user base is always increasing it will result in a more secure cryptocurrency. Since the design of blockchains prevents people from editing the data in the blocks it can be considered tamper-proof. Uniqueness varies from each block because each one can include up to two thousand transactions from millions of users around the world. So, each block will never be the same as the previous one. Their reliability comes from their fixed amount total amount that can be on the market. This amount is set up by algorithms that monitor user productivity. Since it is a decentralized source of money it can stay away from problems that real money has such as it devalues. So, cryptocurrencies are secure from cryptography and financial situations.

What has puzzle-solving to do with cryptography?

If we take a step back from cryptography as a whole, we can make a lot of assumptions that in its entirety, is it similar to puzzle solving. Or turning things into puzzles. Now looking back on cryptography there is a term that is cleverly named cryptograms. This is essentially a puzzle that includes an encrypted text that is then solved to get the plaintext. These are almost minigames using different ciphers to encrypt and decrypt information. These are useful in many different regards including cryptocurrencies. With Bitcoin, they use cryptographic hash puzzles to allow miners to find results and then add them to the blocks which are then added to the blockchain. These cryptographic hashes include a complex algorithm that needs to be solved and then has a fixed output which is stored on the block.

Why have they become popular in cryptocurrencies?

Puzzle-solving has become popular in cryptocurrencies for a multitude of reasons. This is because they provide many beneficial security factors. Such as they are not predictable not one person or machine just inputs a value and achieves the correct output. So, this makes it an even playing field for users of Bitcoin. They are popular because they are one-way functions which means they are nearly irreversible and impossible to reconstruct. With that being said miners' output will never be used again because their output has the designated hash function involved. This is why puzzle-solving has become so popular in the last few years with cryptocurrencies.

What cryptographic techniques that we discussed during the course are being employed in these technologies?

Throughout this course, we covered from the basics to more complex techniques. Some of these are important and are used for things such as cryptocurrencies or website encryption. One of the biggest techniques used in cryptocurrencies that we discussed during our course was symmetric encryption. This is used to take plaintext and result in the ciphertext. Under the umbrella of symmetric encryption, there are many things that we covered such as block ciphers. These are ciphers that encrypt the entire block of plaintext using the same key each time. The second thing that is used in cryptocurrencies that we talked about is asymmetric encryption. This is when we have a public and private key pair. Then anyone and everyone knows the public key but the private key is only known by the owner of it. This is used to authenticate users of cryptocurrencies such as Bitcoin. The third thing we talked about is hashing. There are multiple types and techniques we learned about. In cryptocurrencies, they are used to verify the accuracy of the data in the blocks of a blockchain.

What are the advantages of cryptocurrencies over physical or digital currencies such as credit and debit cards?

One of the most desirable advantages that cryptocurrencies such as Bitcoin have over credit and debit cards is that the transaction fees are minimal. Most people like to save as much money as possible so by using cryptocurrencies they would be saving just a little bit more than their credit or debit card counterparts. Another thing we strive to have is to have a great credit score, this simply does not exist with cryptocurrencies. So, things like interest charges and late fees can negatively impact you. Then there is the factor that the transactions while using Bitcoin are completely anonymous. So, it also provides more privacy to its users than a card with their full name on it. Lastly, another advantage that we discussed extensively in previous paragraphs is that is extremely difficult to hack. There are cryptocurrency scams but they do not devalue or take your actual cryptocurrency, rather it is a credit or debit card associated with an account with cryptocurrency. They both have security risks but things such as Bitcoin are far fewer than its counterpart. Overall cryptocurrencies are more desirable than physical money because of all the reasons we discussed earlier.

Summary of your thoughts on cryptocurrencies---technologies used, advantages, and dangers.

In the world we live in it is difficult to stay off the digital space, there are so many things going on at once that they can be used in countless ways. In the past half-century, we have become so technologically advanced that past civilizations and empires used physical money in elementary. Yes, we still have them today but they do not have the same amount of weight behind them as they once did. We can make thousands of purchases without ever touching or thinking about physical money. I do not think cryptocurrencies will ever go away or replace physical money as we know it. It has its place in the market space and a large supportive community of users around the world. The technologies used to create and maintain cryptocurrencies such as Bitcoin are simply the computers and hardware of the users. Since it operates peer-to-peer there is not one master supercomputer handling the load. It is thousands if not millions of computers used at once to compute its operations. This is called distributed computing. The dangers of cryptocurrencies vary on what is occurring. Anything that involves this amount of technology could be a victim to solar gamma-ray bursts that can take down power grids and distribute all technology involved. This is commonly known and actions are being taken to prevent such cases. Another huge danger with cryptocurrencies is the uninformed population that uses them, this has become prevalent in the social media space. If one such person endorses a cryptocurrency like Bitcoin it can drive up its cost of it dramatically. So, it needs to be noted that all cryptocurrency is volatile and its value comes from its community. Cryptocurrencies are a valuable asset in today's day in age that potentially could revolutionize how we use and trade money forever.

References

A. Lastovetska, "Blockchain architecture explained: How it works & how to build," *Blockchain Architecture Explained: How It Works & How to Build*, 03-Jan-2018. [Online]. Available: https://mlsdev.com/blog/156-how-to-build-your-own-blockchain-architecture. [Accessed: 28-Nov-2022].

A. Siripurapu, "Cryptocurrencies, digital dollars, and the future of money," *Council on Foreign Relations*, 24-Sep-2021. [Online]. Available: https://www.cfr.org/backgrounder/cryptocurrencies-digital-dollars-and-future-money. [Accessed: 28-Nov-2022].

C. Gondek, "Which factors make the blockchain secure?" *OriginStamp*, 2022. [Online]. Available: https://originstamp.com/blog/what-makes-the-blockchain-secure/. [Accessed: 28-Nov-2022].

C. Kusimba Professor of Anthropology, "When – and why – did people first start using money?" *The Conversation*, 13-Sep-2022. [Online]. Available: https://theconversation.com/when-and-why-did-people-first-start-using-money-78887. [Accessed: 28-Nov-2022].

C. Staff, “What is a block in the blockchain? block structure,” *Gemini*, 24-Mar-2022. [Online]. Available: https://www.gemini.com/cryptopedia/what-is-block-in-blockchain-bitcoin-block-size#section-bitcoin-block-headers-and-mining. [Accessed: 28-Nov-2022].

CTGov., “Cryptocurrency risks,” *CT.gov*, 2022. [Online]. Available: https://portal.ct.gov/DOB/Consumer/Consumer-Education/Cryptocurrency-Risks#:~:text=Cryptocurrencies%20aren't%20backed%20by,protections%20as%20a%20bank%20account. [Accessed: 28-Nov-2022].

D. Blystone, “Bitcoin vs. credit card transactions: What's the difference?” *Investopedia*, 20-Feb-2022. [Online]. Available: https://www.investopedia.com/articles/forex/042215/bitcoin-transactions-vs-credit-card-transactions.asp#:~:text=For%20shoppers%2C%20the%20advantages%20of,borrowing%20money%20and%20reward%20points. [Accessed: 28-Nov-2022].

D. Gupta, “Advantages and disadvantages of cryptocurrency in 2020,” *GeeksforGeeks*, 30-Sep-2022. [Online]. Available: https://www.geeksforgeeks.org/advantages-and-disadvantages-of-cryptocurrency-in-2020/. [Accessed: 28-Nov-2022].

D. Rodeck, “What is blockchain?” *Forbes*, 14-Oct-2022. [Online]. Available: https://www.forbes.com/advisor/investing/cryptocurrency/what-is-blockchain/. [Accessed: 28-Nov-2022].

E. Contributors, “Updated 2022 World Currency Symbols, names & codes,” *eurochange*, 25-Oct-2022. [Online]. Available: https://www.eurochange.co.uk/travel/tips/world-currency-abbreviations-symbols-and-codes-travel-money#:~:text=There%20are%20180%20currencies%20in%20the%20world%20circulating%20in%20197%20countries. [Accessed: 28-Nov-2022].

E. Rodriguez, “Alyattes,” *Encyclopædia Britannica*, 12-Nov-2019. [Online]. Available: https://www.britannica.com/biography/Alyattes. [Accessed: 28-Nov-2022].

F. Gogol, “How cryptocurrency gains value -- everything you need to know [2022],” *Stilt Blog*, 15-Nov-2022. [Online]. Available: https://www.stilt.com/blog/2021/07/how-does-cryptocurrency-gain-value/. [Accessed: 28-Nov-2022].

Fluence. sh, “Approaching the problem of eventual consistency in blockchain,” *Medium*, 20-Nov-2018. [Online]. Available: https://medium.com/@fluence.sh/approaching-the-problem-of-eventual-consistency-in-blockchain-950cb443eb36. [Accessed: 28-Nov-2022].

G. Nigeria, “The idea and a brief history of Cryptocurrencies,” *The Guardian Nigeria News - Nigeria and World News*, 26-Dec-2021. [Online]. Available: https://guardian.ng/technology/tech/the-idea-and-a-brief-history-of-cryptocurrencies/. [Accessed: 28-Nov-2022].

H. Buch, “Improving performance & scalability of Blockchain Networks,” *Wipro*, Nov-2019. [Online]. Available: https://www.wipro.com/blogs/hitarshi-buch/improving-performance-and-scalability-of-blockchain-networks/#:~:text=Scalability%20of%20blockchain%20networks%20is,of%20nodes%20in%20the%20network. [Accessed: 28-Nov-2022].

I. Intelligence, “Use cases of blockchain technology in business and life,” *Insider Intelligence*, 15-Apr-2022. [Online]. Available: https://www.insiderintelligence.com/insights/blockchain-technology-applications-use-cases/. [Accessed: 28-Nov-2022].

J. Frankenfield, “Cryptocurrency explained with pros and cons for investment,” *Investopedia*, 22-Nov-2022. [Online]. Available: https://www.investopedia.com/terms/c/cryptocurrency.asp. [Accessed: 28-Nov-2022].

J. Nduati, “Understanding hashing in cryptography,” *Section*, 05-Jan-2021. [Online]. Available: https://www.section.io/engineering-education/understand-hashing-in-cryptography/#:~:text=Hashing%20is%20a%20cryptographic%20technique,you%20get%20the%20same%20outcome. [Accessed: 28-Nov-2022].

J. Royal, “12 most popular types of cryptocurrency,” *Bankrate*, 14-Nov-2022. [Online]. Available: https://www.bankrate.com/investing/types-of-cryptocurrency/. [Accessed: 28-Nov-2022].

K. Szczepanski, “The invention of paper money,” *ThoughtCo*, 17-Oct-2019. [Online]. Available: https://www.thoughtco.com/the-invention-of-paper-money-195167. [Accessed: 28-Nov-2022].

Kaspersky, “What is a cryptocurrency and how does it work?” *www.kaspersky.com*, 09-Feb-2022. [Online]. Available: https://www.kaspersky.com/resource-center/definitions/what-is-cryptocurrency. [Accessed: 28-Nov-2022].

L. Csirmaz, “Cryptography solves old puzzles, creates new ones.,” *Cryptography Solves Old Puzzles, Creates New Ones, Csirmaz Says | Central European University*, 21-Apr-2015. [Online]. Available: https://www.ceu.edu/article/2015-04-21/cryptography-solves-old-puzzles-creates-new-ones-csirmaz-says. [Accessed: 28-Nov-2022].

L. Kuppusamy and J. Rangasamy, “Improved cryptographic puzzle based on modular exponentiation,” *Gwern.net*, 2015. [Online]. Available: https://www.gwern.net/docs/cs/cryptography/2015-kuppusamy.pdf. [Accessed: 28-Nov-2022].

M. B. Team, “Blockchain performance issues and limitations,” *MixBytes*, 22-Jul-2019. [Online]. Available: https://mixbytes.io/blog/blockchain-performance-issues-limitations. [Accessed: 28-Nov-2022].

M. D'Aliessi, “How does the blockchain work?” *Medium*, 04-Jul-2019. [Online]. Available: https://onezero.medium.com/how-does-the-blockchain-work-98c8cd01d2ae#:~:text=To%20be%20added%20to%20the,content%2C%20generate%20a%20defined%20result. [Accessed: 28-Nov-2022].

M.-W. Contributors, “Cryptocurrency definition & meaning,” *Merriam-Webster*, 2014. [Online]. Available: https://www.merriam-webster.com/dictionary/cryptocurrency. [Accessed: 28-Nov-2022].

M.-W. Contributors, “Cryptography definition & meaning,” *Merriam-Webster*, 26-Nov-2022. [Online]. Available: https://www.merriam-webster.com/dictionary/cryptography. [Accessed: 28-Nov-2022].

N. Reiff, “Why should anyone invest in crypto?” *Investopedia*, 20-Feb-2022. [Online]. Available: https://www.investopedia.com/tech/question-why-should-anyone-invest-crypto/#:~:text=A%20Stable%2C%20Censorship%2DResistant%20Store%20of%20Value&text=Unlike%20fiat%20money%2C%20most%20cryptocurrencies,dilute%20their%20value%20through%20inflation. [Accessed: 28-Nov-2022].

n26 Contributors, “Pros and cons of cryptocurrency: A beginner's guide,” *N26*, 14-Sep-2022. [Online]. Available: https://n26.com/en-eu/blog/pros-and-cons-of-cryptocurrency. [Accessed: 28-Nov-2022].

P. de Filippi, “Who controls the blockchain?,” *Homepage*, 31-Jan-2022. [Online]. Available: https://erc.europa.eu/projects-figures/stories/who-controls-blockchain. [Accessed: 28-Nov-2022].

R. de Best, “Number of crypto coins 2013-2022,” *Statista*, 18-Nov-2022. [Online]. Available: https://www.statista.com/statistics/863917/number-crypto-coins-tokens/. [Accessed: 28-Nov-2022].

R. Gaire and S. Nepal, “Cryptographic technique,” *Cryptographic Technique - an overview | ScienceDirect Topics*, 2019. [Online]. Available: https://www.sciencedirect.com/topics/computer-science/cryptographic-technique#:~:text=Cryptographic%20techniques%20are%20used%20to,and%20storage%20of%20the%20data. [Accessed: 28-Nov-2022].

R. Zhang, R. Xue, and L. Liu, “Security and privacy on Blockchain,” *arXiv.org*, 16-Aug-2019. [Online]. Available: https://arxiv.org/abs/1903.07602. [Accessed: 28-Nov-2022].

S. Aggarwal and N. Kumar, “Litecoin,” *Litecoin - an overview | ScienceDirect Topics*, 2021. [Online]. Available: https://www.sciencedirect.com/topics/computer-science/litecoin#:~:text=Litecoin%20(LTC)%20was%20launched%20in,the%20silver%20to%20bitcoin's%20gold. [Accessed: 28-Nov-2022].

S. Contributors, “What is blockchain and how does it work?,” *Synopsys*, 2022. [Online]. Available: https://www.synopsys.com/glossary/what-is-blockchain.html#:~:text=%E2%80%9CEach%20block%20contains%20a%20hash,hash%20of%20the%20previous%20block. [Accessed: 28-Nov-2022].

S. Daley, “Blockchain.,” *BuiltIn*, 01-Sep-2022. [Online]. Available: https://builtin.com/blockchain. [Accessed: 28-Nov-2022].

S. Seth, “Explaining the crypto in cryptocurrency,” *Investopedia*, 08-Jul-2022. [Online]. Available: https://www.investopedia.com/tech/explaining-crypto-cryptocurrency/. [Accessed: 28-Nov-2022].

Synopsys Editorial Team, “What are cryptographic hash functions?,” *Application Security Blog*, 18-Oct-2021. [Online]. Available: https://www.synopsys.com/blogs/software-security/cryptographic-hash-functions/#:~:text=A%20cryptographic%20hash%20function%20is,used%20to%20verify%20the%20user. [Accessed: 28-Nov-2022].

V. Gupta, “Cryptography in Blockchain,” *GeeksforGeeks*, 20-Sep-2022. [Online]. Available: https://www.geeksforgeeks.org/cryptography-in-blockchain/. [Accessed: 28-Nov-2022].

W. Contributors, “David Chaum,” *Wikipedia*, 07-Nov-2022. [Online]. Available: https://en.wikipedia.org/wiki/David_Chaum. [Accessed: 28-Nov-2022].

W. Contributors, “Cryptogram,” *Wikipedia*, 28-Nov-2022. [Online]. Available: https://en.wikipedia.org/wiki/Cryptogram. [Accessed: 28-Nov-2022].

W. Contributors, “History of coins,” *Wikipedia*, 23-Nov-2022. [Online]. Available: https://en.wikipedia.org/wiki/History_of_coins#:~:text=The%20Lydian%20Lion%20coins%20were,the%20value%20of%20the%20contents. [Accessed: 28-Nov-2022].

“What is the world's oldest currency?” *What is the World's Oldest Currency Still in Use? | CMC Markets*. [Online]. Available: https://www.cmcmarkets.com/en/learn-forex/worlds-oldest-currency#:~:text=The%20British%20pound%20is%20the,currencies%E2%80%8B%20in%20the%20world. [Accessed: 28-Nov-2022].

X. Soares, “How blocks are added to a blockchain, explained simply,” *CoinDesk Latest Headlines RSS*, 16-Aug-2022. [Online]. Available: https://www.coindesk.com/learn/how-blocks-are-added-to-a-blockchain-explained-simply/. [Accessed: 28-Nov-2022].