Luke Albert 100/100 100% (A)

CS 463

Cryptography for Cybersecurity

Professor Zehra

 Cryptocurrency is a digital currency based on a network of thousands of computers that is free from third-party interference so it is not being controlled by any government or centralized authority. This is the most important and unique part of cryptocurrency, the decentralization of crypto makes it immune to government control and interference. Cryptocurrency uses the peer-to-peer internet protocol, which allows users to sell and buy directly with another user. Some examples of some cryptocurrencies include Bitcoin, Ethereum, Litecoin, and Dogecoin. Satoshi Nakamoto is the creator of crypto, yet no one knows his or their identity. The very first decentralized cryptocurrency was Bitcoin, which was invented in 2009. Bitcoins initial value is estimated to be about $0.0009 per coin and over the years the value of bitcoin has skyrocketed with the highest value peaking at a record of 68,000 dollars in November 2021. The picture above shows the rate at which bitcoin has grown over the past twelve years from twenty-ten to twenty-twenty-two. Satoshi Nakamoto was not the first person to try and create a digital currency, but he was the one who revolutionized it. Cryptocurrency had some major issues at the beginning such as duplication which was called double-spending. Nakamoto created Blockchain to make this issue go away. Blockchain is a shared recording of transactions across many computers so the transactions cannot be altered without altering every single block on the network. There are many supporters of cryptocurrency some being very high-power and highly supported individuals such as Elon Musk. Cryptocurrency is a digital or virtual currency free from any government control and centralized authority with many different types of cryptos to choose from. There is not much known about the creator and cryptocurrency has been growing more and more in popularity every year. Most cryptocurrencies run on the blockchain network which records transactions on blocks. There are many supporters of this currency and we have not seen the height at which cryptocurrency will achieve. It is still only the beginning of cryptocurrency although with President Biden and inflation crypto has been in the gutters recently.

 Decentralized authority is the best part of cryptocurrency this allows for no government control or interference. It isn’t controlled by one party but yet divided between computers, networks, and nodes. A node is a computer connected to other computers that share information. These nodes are essential to keep cryptocurrency networks functioning. These nodes are connected and send transactions and blocks to each other. Bitcoin can send digital currency securely through the node network. For a new node to join the network it must discover at least one peer to connect with and get a list of other peers from the first peer. The bitcoin client has a list of DNS servers that can give a list of Bitcoin node IP addresses. These nodes can find and connect no matter where the nodes are in the world. Once a node has an IP address of a peer it then goes through an initial handshake with the first message being sent with basic information about itself. The node receiving the message can then can establish a connection by sending back another message. Once a node establishes a connection they can then exchange information with each other such as a list of peer IP addresses. Nodes can leave or join the network at any time. Nodes can also send blocks to any peer missing blocks.

There are four major functions of the bitcoin network, which include routing, storage, mining, and wallet. The routing allows nodes to discover and connect to other peers in the network and also validates transactions and blocks through the network. A node is called a full blockchain node if it stores a copy of the entire blockchain database. This full node can verify any transaction without any external parties so with a full node there is complete independence and freedom from governments and centralized control. A mining node has the purpose to create new blocks or transactions in the blockchain. Bitcoin miners use very powerful computers to solve complex mathematical equations. If these bitcoin miners can solve the equation and successfully add a block to the blockchain then they will receive some bitcoin as payment. The payment for this reward is cut in half after every 210,000 blocks mined. This is to reduce the rate of inflation and pushes the price of bitcoin upward. Currently, each transaction processor and validator are given 6.25 bitcoins for their work. There are 6.25 bitcoins produced in each block and each block is produced roughly every 10 minutes meaning about 900 bitcoins are being produced every day. Anyone with a computer can mine bitcoin if they download one of the many bitcoin mining services out there, but it requires some powerful equipment for any actual results. It is very expensive to be able to mine bitcoin because the more powerful the computer the more equations will be able to be solved so if a slow beat up computer is trying to mine bitcoin it is never going to be able to out mine the strong supercomputers built solely for mining bitcoin.

 Cryptocurrencies can be used and exchanged due to the blockchain. I have written a little about the blockchain earlier, but I am going to go into more detail. The blockchain is a digital database or ledger that is distributed between the nodes on the peer-to-peer network. Due to this blockchain people can buy or sell transactions without having to go through a centralized authority. This gives people more freedom with their money. Blockchains have many pros such as increased transparency, accurate tracking, permanent ledger, and cost reduction. The blockchain allows users to save money by lowering transaction costs. Due to no centralized authentication, it is a peer-to-peer network so there is not a big third-party transaction cost. After a transaction is processed a new block will be added to the blockchain forever in a way that is permanent and unchangeable. Blockchain can solve a lot of issues in the world such as blockchain in supply chain management. This would allow consumers to see where their products and supplies are coming from. This will prevent waste, inefficiency, fraud, and unethical practices. Blockchain is also useful to keep track of charities spending their money ethically and in a charitable way. This will make it so charities can’t just take all of the money and spend it for themselves and donators can see exactly what their money was spent on and where it went. Blockchain can prevent fraud, waste, and unethical doings by tracking the money spent. Blockchains provide transparency making it difficult to corrupt and manipulate.

Blockchain is immune to hacking unless the attacker has over fifty percent of the blockchain’s computational power. This computational power is called a hash rate, and if the attacker owns over half or fifty percent of the blockchain hash rate then they can then manipulate the network and make changes to transactions. This attack would be called a fifty-one percent attack. Once it occurs, all of the pending transactions that have not been processed yet can be reversed. The attackers can then transfer those transactions to anywhere else and wire the transaction to themselves, altering the blockchain. Blockchain isn’t run by one person but everyone who uses it technically owns it. One of the biggest problems with blockchain is its scalability. Blockchains are hard to scale and the larger the blockchain the harder it is to scale. The blockchain will keep increasing forever and users do not need to store the entire blockchain to use it. blockchain technology is very secure and prevents hacking or being shut down. The blockchain is good for transparency in the verification and traceability of transactions. Blockchain increases trust and security and eliminates any need for a centralized authority or government intervention.

 Blockchain is not only relevant to cryptocurrencies, but it is also relevant in many other areas. Blockchain can be used in financial services, healthcare, government, travel, hospitality, retail, and consumer goods. Blockchain can be useful for money transfers due to other money-transferring systems require a large fee and can take multiple days or even weeks to transfer money. Blockchain transactions can take minutes or even seconds with a reduced fee to transfer money. This allows for faster and cheaper transaction costs. Blockchain can also help with insurance by not allowing customers to make duplicate claims for the same event preventing insurance fraud. Blockchain would also allow customers to receive their claim payments faster than without blockchain. Blockchain technology is also useful for real estate. Real estate causes a lot of files and paperwork to confirm financial information and ownership. With blockchain, it would create a faster, more secure, and more accessible way of getting that verification and ownership. This would make real estate transactions move faster, reduce the amount of paperwork needing to be done and it would save a lot of money. Blockchain could also be used for voting. Voting has been a hot topic in the United States with conspiracies of the 2016 and 2020 elections being rigged. If we used blockchain to vote then it would confirm that no one would be able to vote twice, it would make sure that only eligible voters are allowed to vote and the votes would not be able to be tampered with. Due to the blockchain being unchangeable the votes would be sealed and wouldn’t be tampered with like the conspiracies of the 2020 election claim. Blockchain can also help artists and songwriters get paid for their work. With the internet, many people can steal artists’ hard work and copy and post them online for their own gain. Blockchain was created so the same file cannot exist in more than one place so the artists would get paid what they should be getting paid. Non-fungible tokens or NFTs can also benefit from blockchain as NFTs are digital art. This would allow the NFT owner to completely own the art and now allow any other copies of the art to exist. This would make NFTs similar to collecting physical art. Blockchain allows verification and security of transactions.

 Cryptocurrencies are secure, reliable, tamperproof, and unique. Cryptocurrency uses encryption to verify its transactions and is secured through the use of personal keys. Cryptocurrency is very reliable due to its lack of government and centralized authority intervention. It is also completely digital so in the event of a social collapse, the user will always have their currency online. If a government destroys the value of their dollar and puts restrictions on the citizen’s money they would be fine if they had invested in cryptocurrency. Cryptocurrencies are tamperproof due to the blockchain which posts every single transaction with when it happened as well. This is all very unique because there has never been a currency that is so volatile, secure, and transparent.

 Puzzle-solving has become popular in cryptocurrency because this is how bitcoin and cryptocurrencies are mined and created. These cryptographic hash puzzles are complex equations to verify blocks of the transaction on the blockchain. Solving these puzzles is not like solving a normal mathematical equation. The puzzles require an insane amount of computing power and very expensive equipment. However, these puzzles aren’t solved with no monetary gain. For each puzzle solved the solver will get 6.25 bitcoin. Which currently would equal $106,985 US dollars, and at the peak of bitcoin it would equal a whopping $425,000 US dollars. It can be completely worth it to solve these puzzles and equations but more than likely it is unable to be supported because mining requires top-notch equipment and computers.

 There are many advantages cryptocurrency has over physical currencies. To begin the transaction cost is very low. Anyone can use cryptocurrency as opposed to setting up a bank account which requires pages of documentation and paperwork. International cryptocurrency transactions are faster than wire transfers as well. Cryptocurrencies allow 24/7 access to money with no limits on withdrawals or purchases. A bank failure is one of the reasons the United States went into the Great Depression, and without having to rely on banks if a bank failure and Great Depression ever occurred again. Those with cryptocurrency wallets will be sitting just fine, and not have to wait in a long busy line to be denied money like the people in the photo below. 

 Cryptocurrency transactions act like a cash transactions by immediately pushing a transaction through by not needing to go through a third-party institution such as a bank. Cryptocurrencies are stored in a digital wallet that the user holds and controls. There the money is in the hands of the user and instead of using a debit card and the money is in the hands of the bank. Cryptocurrency transactions are processed almost immediately and use the currency in the wallet as opposed to a credit card which is like a temporary loan from the bank. Cryptocurrency is more secure, safer, and reliable than banks which often do not have twenty-four-seven availability.

 There is not much known about the creator of cryptocurrency and bitcoin there are only speculations of who the man or woman may be. Satoshi Nakamoto is the man who created such a wonderful and ingenious invention. His name itself is a fictional name or a pseudonym. Reports say that Nakamoto was active in the creation of Bitcoin and Blockchain in 2010 but has not been heard of since. There are speculations and internet rumors about who the mysterious Nakamoto is. Some names of who he could be are Dorian Nakamoto, Craig Wright, Half Finney, and Nick Szabo. Although these are just speculations all have suspicions of being the man himself Satoshi Nakamoto. Satoshi Nakamoto could also have passed away or just simply does not want to deal with the fame that is going to come with being Bitcoins CEO and founder.

 Cryptocurrency is the future of currency while everything is transitioning online so are our payment systems. The best online payment system is a cryptocurrency where the currency is completely virtual and online. Cryptocurrency can be useful to avoid unnecessary expensive processing fees to save users money. It also is safe and secure while having no centralized government that is able to gain control of the people’s money. It is also popular to try and make money off cryptocurrency as the prices can trend upward or downward people will try to buy a specific cryptocurrency when it costs low and sell when it costs a lot. The early investors of bitcoin are all millionaires besides those who got out too early. Cryptocurrency is self-governed, secure, protected from inflation, has faster and cheaper transactions, and the best part it is decentralized.

References:

A. Hayes, “Who is Satoshi Nakamoto?,” *Investopedia*, 28-Sep-2022. [Online]. Available: https://www.investopedia.com/terms/s/satoshi-nakamoto.asp#:~:text=Satoshi%20Nakamoto%20is%20a%20pseudonym,not%20been%20heard%20from%20since. [Accessed: 30-Nov-2022].

G. Arroyo, V. Díaz, and E. Hernández, “Blockchain,” *Amazon*, 2019. [Online]. Available: https://aws.amazon.com/blockchain/blockchain-for-supply-chain-track-and-trace/#:~:text=With%20blockchain%2C%20supply%20chain%20companies,at%20any%20point%20in%20time. [Accessed: 30-Nov-2022].

J. Edwards, “Bitcoin’s price history,” *Investopedia*, 22-Nov-2022. [Online]. Available: https://www.investopedia.com/articles/forex/121815/bitcoins-price-history.asp. [Accessed: 30-Nov-2022].

M. Yano, C. Dai, K. Masuda, and Y. Kishimoto, “Blockchain and Crypto Currency [electronic resource] Building a High Quality Marketplace for Crypto Data,” Singapore : Springer Singapore : Imprint: Springer, 2020.

S. Arora, “What is cryptocurrency: Types, benefits, history and more [2022 edition]: Simplilearn,” *Simplilearn.com*, 31-Oct-2022. [Online]. Available: https://www.simplilearn.com/tutorials/blockchain-tutorial/what-is-cryptocurrency#:~:text=will%20be%20produced.-,Benefits%20of%20Cryptocurrency,limits%20on%20purchases%20and%20withdrawals. [Accessed: 30-Nov-2022].

S. McGee, “How bank failures contributed to the Great Depression,” *History.com*, 13-May-2021. [Online]. Available: https://www.history.com/news/bank-failures-great-depression-1929-crash. [Accessed: 30-Nov-2022].