Course Paper: Cryptocurrency

Alexander Gardner

Old Dominion University

What are cryptocurrencies?

Cryptocurrency can best be explained when splitting it into two words, crypto and currency. When it comes to the word crypto this "refers to the various encryption algorithms and cryptographic techniques that safeguard entries, such as elliptical curve encryption, public-private key pairs, and hashing functions [1]." Then when we move over to currency this shows that it is also used as "a form of digital asset based on a network that is distributed across a large number of computers [1]."

Another key factor to note in the world that is cryptocurrency is that it is decentralized and completely outside of the control of any government or central authority [1]. This comes with its pros and cons though. On the pro side this enables cheaper and faster money transfers, and the decentralized systems also does not collapse due to a single point of failure [1]. On the other hand, this factor breeds an environment for extremely volatile prices, high energy costs for mining activities, and its use for criminal activity [1].

One may wonder what these mining activities are though. Cryptocurrency "mining is the process by which transactions are verified on the blockchain" and is performed using "hardware and software to generate a cryptographic number that matches criteria. [2]" Miners serve as the auditors in the crypto world [2]. To incentivize users to mine and serve as auditors in the crypto world they are rewarded with a crypto coin when they generate the cryptographic numbers and solve the equation by matching it with the criteria [2].

What are some examples of cryptocurrencies?

In today's day and age, there are around 10,748 cryptocurrencies with a total market cap of $1.32 trillion [3]. The most popular and oldest cryptocurrency today is Bitcoin. Bitcoin also known as BTC, has a total market cap of $721.2 billion and a single Bitcoin cost around $36,894 [4]. Bitcoin runs on a "a ledger logging transactions distributed across a network of thousands of computers. Because additions to the distributed ledgers must be verified by solving a cryptographic puzzle, a process called proof of work, Bitcoin is kept secure and safe from fraudsters. [4]" The next most popular coin on the market is Ethereum with a market cap of $239.8 billion [4]. Ethereum just so happens to not only be a cryptocurrency, but it is also a blockchain platform [4]. One of the most attractive features of Ethereum is the Ethereum Virtual Machine which allows programmers can run and create programs on a decentralized platform, create smart contracts, cryptographic tokens, and a host of other resources [5]. Coming in third on the world stage of cryptocurrencies is Tether with a market cap of $88.1 billion [4]. This cryptocurrency is a stablecoin meaning that it is backed by fiat currencies like the US dollar or Euro [4].

One popular phenomenon in today's crypto world though is the Meme coin. These coins serve no purpose and have no value, but still garner attention. Meme coins are created as a joke based around a popular meme or internet joke circulating the internet. One popular example of this is the Dogecoin which reached a market cap of $88 billion following an endorsement from the notorious Elon Musk [6].

What is a blockchain?

The blockchain serves as a ledger to maintain a secure and accurate record of transactions for a cryptocurrency [7]. Although blockchains are most commonly referred to in the context of cryptocurrencies they also have a purpose outside of it. As a matter of fact, blockchains can be used to make any set of data immutable or in other words the data cannot be altered [7]. One may wonder how this blockchain works though. The blockchain is like a traditional database or spreadsheet, but its structure and the way you access it is different. Every action a user would

normally do like viewing or entering information is accomplished using scripts [7]. An additional attribute of blockchains that make them particularly fantastic is that they are distributed which means multiple copies of the database are stored on multiple machines, and all copies need to match for it to be valid [7].

What is in the block of a blockchain?

When we take a closer look at the blockchain we can see that it stores its information into blocks. Much like in a spreadsheet, each cell is a block [7]. A block is a data structure where a cryptocurrency transaction data is permanently stored [8]. Most blocks include several elements including the magic number, blocksize, block header, transaction counter, and transactions [8]. The magic number holds a specific value which determine which determines which cryptocurrency network the block belongs to [8]. The blocksize sets the maximum size for a block so that only a certain amount of information can be placed into the block [8]. A block header holds the information about the block [8]. Each blockhead "contains information about the block itself (block metadata), typically including a timestamp, a hash representation of the block data, the hash of the previous block's header, and a cryptographic nonce (if needed) [9]."

How are the blocks linked?

*******Due to the distributed nature of the blockchain these blocks need to be linked together into a chain. This achieved with the cryptographic technique of hashes. Each block contains the hash of the previous block, timestamp, and transaction data. *****

When are the blocks added?

Blocks are permanently added to the blockchain through a complex process called mining. The process of mining involves a network of computers each communicating with each other through a peer-to-peer network each solving complex math equations. Once these equations are solved a transaction is confirmed and a block is added [10]. To accomplish this, miners use two common methods: proof-of-work and proof-of-state [11].

Proof-of-work is used by two of the most popular cryptocurrencies, Bitcoin and Ethereum. This algorithm aims to set each miner against each other in a competition to compete for a cryptocurrency reward. The competition takes place on a machine running an intense program each trying to be the first to solve a complex math problem. To find the winning proof-of-work miners try to find a hash with a matching number of leading zeroes with the current target hash [12]. This rigorous battle comes to an end once every 10 minutes and once the target hash is matched a new block can be added to the blockchain [12].

The main reason for the proof-of-work algorithm and system is to secure a cryptocurrency and prevent users from printing extra coins they did not earn [13]. In other currencies this is not an issue because there is one central authority. For example, we cannot double spend a dollar on a debt card because there is a bank tracking the transactions and ensuring the integrity of said transactions. Proof-of-work solves this issue because the process of finding the matching hash is difficult enough to prevent the manipulation of transaction records, but verifying the hash is not [10]. While this sounds reasonable it does not come without any downsides. One of the major issues with the proof-of-work algorithm is the high energy usage needed to make it work. Some estimates set the total power usage of proof-of-work mining to be as high as the entire country of Switzerland [13]. Another key issue with the proof-of-work scheme is the inequality in the competition. Only three mining pools control nearly 50% of all the computational power [13].

The next method, proof-of-stake, aims to fix this issue by reducing the energy usage for verifying transactions and adding blocks to the blockchain in addition to leveling the playing

field for miners. Proof-of-stake is also used to verify transactions and add blocks to the blockchain, but it does so by giving users the option to stake their cryptocurrency. When a transaction is ready, a validator node reviews the block. If the transactions in the block are accurate the block is added, and crypto rewards are given to the miners who put up their cryptocurrency and if it is not, they lose a portion of their stake.

Who adds the blocks – centralized server or distributed servers? Who maintains the blockchain?

Part of the beauty of cryptocurrency is the fact that it is run with a decentralized infrastructure with distributed servers. No one person or organization can control the blockchain, the power of the blockchain lies in the hands of the people. The people verify the transactions and add the blocks. The people maintain the blockchain.

Are these scalable? In other words, can the chains be as long as you wish them to be? What are the performance implications of having long chains?

With over 425 million cryptocurrency users and a growth of 8,000% since 2016 one may wonder how well the blockchain can scale [14]. The size of the Bitcoin blockchain has grown from 614 megabytes in 2012 all the way to 250 gigabytes of data that each peer on the blockchain carries [15]. With more and more users exponentially fueling the growth of the blockchain the scalability issues have been brought to the forefront. The core of these issues can all point to the fact that to process each transaction needs to be verified by a complex mathematical equation. As more and more transactions come through the longer it will take to get them confirmed, added, and processed. In theory the blockchain's size is infinite and only limited by the hardware of our current technology.

How is consistency maintained among copies of blockchains?

The blockchain maintains consistency amongst the copies by making the blockchain immutable and a consensus protocol. One cannot delete or modify the chain without a consensus from the network [16]. Also, to ensure that unauthorized transaction entries the blockchain has methods like the proof-of-work and proof-of-stake algorithms to maintain consistency.

Examples applications where blockchain technologies are being used.

One application taking advantage of blockchain technologies in use right now is smart contracts which take advantage of Ethereum technology. "A smart contract is a self-executing program that automates the actions required in an agreement or contract. Once completed, the transactions are trackable and irreversible [17]." Smart contracts completely remove the need for third parties thus speeding up contract executions, completely removing human error from the third party, and ensures the integrity of a contract because these contracts are immutable [17]. On the flip side though, these positives can sometimes become a negative. Smart contracts being immutable means if there is a mistake in the coding of the contract or a loophole is in it, they cannot be changed [17].

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

Cryptocurrency takes advantage of cryptographic techniques like asymmetric cryptography and hashing. When it comes to asymmetric cryptography, cryptocurrencies take advantage of this method to manage addresses on the blockchain [18]. Cryptocurrencies help manage the blockchain by using key pairs where the public key view the address and the private key is used to access and authorize action at the address [18]. Hashing also comes in handy in the blockchain. Solving a hash is the root of cryptocurrency mining and securing the entire blockchain.

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

The main draw of cryptocurrencies is that it exists outside the control of any government or organization. This makes cryptocurrency accessible for everyone and gives an air of transparency to the entire operation. Another advantage that comes with cryptocurrency is faster transaction speeds and costs. Most wire transfer that goes through the U.S. financial institutions takes around 24 hours to go through and can cost $25 to $30 dollars [19]. With cryptocurrencies a wire transfer takes a matter of minute with substantially less costs [19].

Conclusion

Cryptocurrency aims to revolutionize currency. Cryptocurrency aims to bring us into a world where currency is not control by any bank, government, or organization. The currency lies in the hands of the people. While this sounds great it does not come without its dangers. The price is insanely volatile, and the scheme is vulnerable to a 51% attack. If a group of miners or an organization control more than 50% of a network's mining hash rate they can alter the blockchain [20]. In a sense if anyone controls 51% of a network's hash rate, they control the blockchain. Cryptocurrency and blockchain technology are used across many industries like the supply chain, medical, finance, and more. Some may see it is the technology of the future.

References

[1 J. Frankenfield, "Cryptocurrency Explained With Pros and Cons for Investment," 2 November 2023. [Online]. Available: https://www.investopedia.com/terms/c/cryptocurrency.asp.

[2 E. Hong, "Investopedia," 18 October 2023. [Online]. Available: https://www.investopedia.com/tech/how-does-bitcoin-mining-work/.

[3 J. Howarth, "How many cryptocurrencies are there in 2024?," ExplodingTopics, 3 November 2023. [Online]. Available: https://explodingtopics.com/blog/number-of-cryptocurrencies.

[4 K. Tretina, "Top 10 Cryptocurrencies of November 2023," Forbes, 21 November 2023. [Online]. Available: https://www.forbes.com/advisor/investing/cryptocurrency/top-10-cryptocurrencies/.

[5 A. Davies, "Why Blockchain Developers Use Ethereum?," DevTeam.space, [Online]. Available: https://www.devteam.space/blog/blockchain-developers-use-ethereum/.

[6 D. Ashmore, "What are Meme Coins? Are They Worth Investing In?," Forbes Advisor, 4 August 2022. [Online]. Available: https://www.forbes.com/advisor/investing/cryptocurrency/what-are-meme-coins-are-they-worth-investing-in/.

[7 A. Hayes, "Blockchain Facts: What Is It, How It Works, and How It Can Be Used.," Investopedia, 23 April 2023. [Online]. Available: https://www.investopedia.com/terms/b/blockchain.asp.

[8 J. Frankenfield, "What is a Block in the Crypto Blockchain, and How Does it Work?," Investopedia, 9 January 2022. [Online]. Available: https://www.investopedia.com/terms/b/block-bitcoin-block.asp.

[9 D. Yaga, P. Mell, N. Roby and K. Scarfone, "Blockchain Technology Overview," NISTIR, 2018.

[1 L. Daly, "What Is Proof of Work (PoW) in Crypto?," The Motley Fool, 17 November 2023. [Online]. Available: https://www.fool.com/terms/p/proof-of-work/#:~:text=The%20proof%2Dof%2Dwork%20model%20is%20a%20consensus%20mechanism%20used,transactions%20has%20a%20specific%20hash..

[1 X. Soares, "How Blocks Are Added to a Blockchain, Explained Simply," Coindesk, 2023 May 2023. [Online]. Available: https://www.coindesk.com/learn/how-blocks-are-added-to-a-blockchain-explained-simply/.

[1 S. Harisakthi, "How Blocks are Created in Blockchain?," LinkedIN, 2 May 2023. [Online]. Available: https://www.linkedin.com/pulse/how-blocks-created-blockchain-sindhu-harisakthi#:~:text=The%20process%20of%20creating%20a,next%20block%20to%20the%20blockchain..

[1 A. Hertig, "What is proof-of-work," Coindesk, 12 January 2023. [Online]. Available: https://www.coindesk.com/learn/what-is-proof-of-work/.

[1 J. Howarth, "75+ Incredible Cryptocurrency Statistics (2023)," Exploding Topics, 11 October 2023. [Online]. Available: https://explodingtopics.com/blog/cryptocurrency-stats.

[1 1. Blockchains, "Blockchain Size: Everything You Need to Know," 16 September 2021. [Online]. Available: https://101blockchains.com/blockchain-size/.

[1 "What is Blockchain Technology?," AWS, [Online]. Available: https://aws.amazon.com/what-is/blockchain/?aws-products-all.sort-by=item.additionalFields.productNameLowercase&aws-products-all.sort-order=asc.

[1 J. Frankenfield, "What Are Smart Contracts on the Blockchain and How They Work," Investopedia, 31 May 2023. [Online]. Available: https://www.investopedia.com/terms/s/smart-contracts.asp.

[1 blockgenic, "Asymmetric Cryptography In Blockchains," Hackernoon, 22 November 2018. [Online]. Available: https://hackernoon.com/asymmetric-cryptography-in-blockchains-d1a4c1654a71.

[1 A. Levy, "Why Should You Use Crypto?," The Motley Fool, 14 November 2023. [Online]. Available: https://www.fool.com/investing/stock-market/market-sectors/financials/cryptocurrency-stocks/benefits-of-cryptocurrency/.

[2 J. Frankenfield, "51% Attack: Definition, Who Is At Risk, Example, and Cost," Investopedia, 7 June 2023. [Online]. Available: https://www.investopedia.com/terms/1/51-attack.asp.

[2 J. Cornfield, "Money.com," 21 February 2023. [Online]. Available: https://money.com/what-is-cryptography/#:~:text=Cryptography%20allows%20cryptocurrency%20transactions%20to,on%20a%20third%2Dparty%20intermediary..

[2 J. Royal and B. Baker, "12 Most Popular types of cryptocurrency," 7 November 2023. [Online]. Available: https://www.bankrate.com/investing/types-of-cryptocurrency/.

[2 S. Nevil, "What is Proof of Work in Blockchain," Investopedia, 27 May 2023. [Online]. Available: https://www.investopedia.com/terms/p/proof-work.asp.