Blockchain

By Carlos Perches and Ethan Sandman

CS395

Abstract

This paper explores the evolution and impact of blockchain technology. It goes over the key foundational principles of blockchain such as its immutability, its decentralization, smart contracts and decentralized finance (DeFi). This paper also addresses some pitfalls of blockchain, that being its poor efficiency, its scalability, and redundancy. With Blockchain being the backbone of cryptocurrencies and NFTs, this paper addresses how crypto currencies utilize Blockchain in terms of its secure network, transparency and more. NFTs are another big factor of blockchain and also utilize many of blockchains basic functions. It explains how NFTs are not fungible and how each NFT is unique along with many of its drawbacks being how NFTs can be tampered with, spoofed, and much more. This paper gives a general overview of blockchain along with its pitfalls.

Introduction

Blockchain dates back all the way to the late 1980s when two scientists by name of Stuart Haber and Scott Stornetta developed a “time-stamping structure" which we all refer to as blockchain nowadays (Whitaker 6). They shared a concern that many of us till this day share, which is how can we make sure all transactions are safe and secure. They wanted to make sure that everyone had access to past transactions to verify who was telling the truth and to help avoid fraud (Whitaker 6). Blockchain is still an up and coming piece of technology that will continue to grow. Back in 2008, which is when Blockchain “officially” started. It started with an anonymous group or person for that matter, that released a paper called “Bitcoin: A Peer-to-Peer Electronic Cash System” (van den Berg 1). The paper presents a detailed justification for this technology, emphasizing its pivotal role in bolstering security measures and enabling the direct transfer of electronic funds without requiring intermediary supervision. A year later in 2009 the first ever cryptocurrency known as Bitcoin was released. At first Bitcoin was just another piece of random code on the web but with its open-source, coders around the world began to refine it and improve upon it (Luther 1). Over the years Bitcoin has dramatically risen in value to thousands of dollars just for one Bitcoin. Cryptocurrencies are a new form of online

transactions, that can take the form of almost anything. Cryptocurrencies are new, and mostly used by people looking to make a quick buck. The problem with cryptocurrencies is that the moment of when to buy or sell changes quickly, so it is difficult for new investors and even experienced ones to determine when the best moment to buy is. Cryptocurrencies use Blockchain, which is the foundation for all microtransactions. Cryptocurrencies rely on blockchain as a digital ledger and to use blockchain, they use a method called mining. “Mining adds records of past records to the distributed ledger of blockchain (IEEE, Abstract, 2016),” mining is the way that blockchain accesses information dug up by each new user. Blockchain also led to the upbringing of NFTs (non-fungible tokens). NFTs have been around since 2014 with the first ever NFT “Quantum” being minted by Kevin McCoy in 2014 (Murray 26). NFTs only really started to gain popularity, back in 2017 with the game called “CryptoKitties”. This game promoted the new standard at the time ERC-721, one of many standards for NFTs (Wang 2). Blockchain, cryptocurrency and NFTs are only bound to keep growing in the coming years as they continue to gain popularity around the world.

Blockchain

Blockchain is a new concept that over the years has continued to grow and be improved upon. Blockchain is a relatively simple concept of how it works. The overall view is that it’s a chain of blocks, hence the name, each block being a separate transaction of an NFT or anything else for that matter, with each block having its own unique hash (Nakamoto 2). With the idea being that once a block is added to the chain it cannot be removed, edited, or changed in any way. This brings up the concept of the blockchain being “immutable” (Murray 28). Blockchain being immutable is what separates it from other ledgers out there. The key difference is that other ledgers have a central authority whether that be the government, the bank or anything else. This means that you solely rely on the central authority to be truthful about all the logged transactions (Whitaker 3). The ledgers owner would be able to modify any previous transactions in order to help them with their current business/ their interests (Crumpler 3). With blockchain, everyone using the blockchain would be able to see all transactions from day

one. With Blockchain being immutable, it doesn't allow for anyone to modify these blocks/transactions that have occurred in the chain. This allows for greater transparency for everyone using the blockchain (Crumpler 3). This also helps prevent any attacks from a hacker or a single bad node, node also being one of the users of the blockchain. Since everyone has a copy of the blockchain a hacker would have to hack into hundreds if not thousands of people to manipulate past transactions. This is very unlikely to happen and probably not possible (Murray 31). This brings up the topic of Blockchains resiliency to attacks. The large size of blockchain gives it an advantage when it comes to hackers. Even with natural disasters, if the blockchains network is geographically diverse enough, it will continue to operate fine without any interruptions. Private Blockchains are a little more susceptible to attacks and damage from natural disasters but still tend to be resilient (Crumpler 6).

Smart Contracts

Smart contracts try to help limit fraud that happens between two parties that are in the middle of a transaction. Smart contracts are coded contracts that when all requirements by both parties are met and agreed upon automatically executes the transaction. This is beneficial for parties that do not trust one another. It also gets rid of the need for a third party to manage these exchanges. This reduces the cost of transactions and greatly increases the speed as well. Although these also come with some risk as well. One being that false information can be uploaded to the blockchain which can cause some smart contracts to trigger (Crumpler 8).

DeFi (Decentralized Finance)

DeFi is a new concept that tries to solve a lot of issues involved with financial services. DeFi makes use of blockchain by not having a central authority controlling the network along with any transaction. DeFi is supposed to be a service that can lend money to people, investing, insuring and many more. It's basically trying to be a bank but without all the governance (Dekker 1). Everything about DeFi is also supposed to be open, meaning that anyone with an internet connection would be able to take advantage of DeFi. DeFi also makes use of smart contracts like Blockchain. This allows for quick and secure transactions between parties. DeFi

has all the benefits of blockchain being fully transparent, high security, immutability along with much more (Dekker 2). The unfortunate thing is that DeFi is far from being complete. DeFi is still a very new concept that still needs trial and error as it continues to reach issues with scalability, optimization, which are just to name a few (Dekker 2).

Drawbacks of Blockchain

Blockchain also has many drawbacks with it, some being its poor efficiency, scaling, redundancy, which are just to name a few. With redundancy this can be very cost and time consuming. With every transaction that happens on blockchain, being recorded to every node on that chain. Many times, this can be pointless as many transactions are insignificant and don't necessarily need to be shared with everyone. This also increases the cost of operating each blockchain (Ammous 4). This also limits the size of the data stored on blockchain. These limitations are in place as every node needs to be able to store a copy of every transaction that has occurred. If files that were being stored on the blockchain were allowed to be any size, the blockchain we quickly run into storage issues and blockchain already being as slow as it is, would run much slower (Crumpler 7). To put into perspective of how slow blockchain actually runs, the VISA network is able to clear 400x as many transactions per second compared to a Bitcoin transaction taking place on the blockchain. For a single Bitcoin transaction, it takes equivalent amounts of energy for 770,000 VISA transactions (Crumpler 7). These time complexities usually only apply to public Blockchains and not private ones. Since private ones are usually much smaller in comparison, this will greatly increase its speed and its energy consumption closer to traditional ledgers (Crumpler 7). Irreversibility can also be a drawback of blockchain. Main reason being that any simple mistake that as made in a transaction will be a mess to fix. In a traditional ledger, any mistake that was made during the transaction can easily be fixed and corrected. Things are not so simple when it comes to the blockchain. To fix a mistake on blockchain you need to do what's called a "hard fork". This is where you have to use 51% of the network's processing power to get all the nodes to agree to move to an appended blockchain (Ammous 4). This method often doesn't work with larger blockchains as the cost of all the resources it takes to do this often doesn't out ways the gain. Also getting all the nodes to agree to the appended blockchain is not likely. Scaling is also another issue with blockchain.

Often the transaction ledger will grow faster than the blockchains members, causing each member to face storage and computational issues.

Cryptocurrency

What are cryptocurrencies? Well, cryptocurrencies are a "peer-to-peer digital exchange system in which cryptography is used (IEEE, 2016)." Cryptography is used to generate and distribute the currency of each type of cryptocurrency. Cryptocurrencies were made to get rid of the central transaction system that banks use. The transactions are made to be simple and easy to transfer from one account to another. The only way to confirm the transaction is through the verification process. The verification process confirms transaction amounts, whether the user owns the account or is looking to make a new one. The process of using the verification process is called mining. Each type of cryptocurrency uses a different type of mining technology that adapts to each of their own form of transaction. Some cryptocurrencies focus on restricting the transactions made during a certain amount of time, while others focus on achieving fast lightweight services (IEEE, 2016).

There are many types of cryptocurrencies used for all number of transactions. There are types of cryptocurrencies that everyone should have heard of, such as Bitcoin and Ethereum. These currencies are similar as they are traded through online exchanges and are stored in various types of cryptocurrency wallets (Reiff, Investopedia). Even though these two currencies may be similar in how they trade, but the structure of these currencies couldn't be more different. Bitcoin is made to provide an alternative to physical currency, and get rid of the use of banks, while Ethereum is made for complex smart contracts and decentralized applications. Bitcoin was the start of cryptocurrencies, it was introduced as an online currency without any central

authority, like all physical based currency that is backed by governments, they are not physical and is kept track of using the public digital ledger. Ethereum is the largest open-ended decentralized software platform. Ethereum uses smart contracts and decentralized applications without downtime, fraud control, or interference from a third party (Reiff, Investopedia). Ethereum can accomplish this using blockchain. Ethereum uses its own form of currency known as ether. Ether has four main uses, it is traded as currency, held for investments, used to purchase goods and services, and they are used on the Ethereum network to pay the transaction fees.

Pros and Cons of Cryptocurrency

There are many pros towards the use of cryptocurrency. One of these pros would be the increase in popularity of cryptocurrencies leading investors to wanting to buy into them and invest their money into something that will gain a profit. Bitcoin is the most popular for a reason, since it is easy to use, and the transfer of money is simple without the hassle of using banks and other financial companies. The transaction speed is handy as there are no difficulties, and all transactions are made within a couple of minutes of the start of the transfer. Many people are fond of this since with physical currency, there are draw backs and many ways for the transfer to take longer. These transactions are also very cost effective, with the transaction fee being minimal or even nothing at all. This is great as it eliminates the need for third parties to confirm transactions. Investors also like that these transactions are kept protected and private. There is no third-party intervention, so their account is kept secure and only accessible to them.

A downside for using cryptocurrency is that they claim to be anonymous in their transactions, but in reality, there is a digital trail left behind. Blockchain is still not totally secure, as there is a 51% risk of attack where the miner can take control. This problem can lead to the miners to double spend coins, prevent new transactions, and more (). But this problem is only

seen in newly formed blockchains which need time to work out their kinks. There is also a lack of key policies which is a big drawback for cryptocurrencies. There are no refunds, or cancellation policies that people can use to get their money back. It is all about when the best time to buy or sell is to get the full extent of a profit.

Mining (proof of work)

Every cryptocurrency uses the technology known as blockchain. Using blockchain, a transaction is made by two users and through that transaction, it is validated by mining. Mining validates the transaction and adds them to the digital ledger held by blockchain. Mining is a brute-force algorithm and should be designed so that the number of blocks mined per day remains constant to control the rate of introduction to new currencies, which are unlocked when a block is mined (IEEE, 2016). Cryptocurrencies mine with one-way functions also known as hashes. The miner gets the hash from previous blocks as an input and would have to choose a nonce, and when the current hash and the nonce are hashed, the following structure is defined by the cryptocurrency. Calculating the input from a hash is resource intensive, but verifying its correctness is fast. Mining is needed to use cryptocurrencies, but it also has its problems as it is not perfect, as there are mining attacks that affect newer blocks.

NFTs (Non-fungible Tokens)

NFTs were first used in 2012, when Bitcoin introduced “Colored Coins” (Valeonti 3). NFTs are a type of cryptocurrency but instead are non-fungible. This means that you cannot exchange a NFT for another at the same price, like you could with bitcoin since all bitcoins are equivalent in value. NFTs gained popularity and their traditional format with the release of the

ERC-721 standard and has continued to improve on that standard with the newer ERC-1155 (Wang 1). NFTs ae a way for people to prove ownership of online property. This can be in the form of online paintings, virtual real estate, videos, and many more things. NFTs were derived from Ethereum smart contracts, which is why most NFTs use the Ethereum blockchain. This gets all the benefits of blockchain by allowing users to see the full history of transactions with the NFT that they are looking at and also allows them to verify ownership.

How do NFTs Work?

Every NFT has a unique identifier that is placed into a blockchain. This became standard with the release of the standard ERC-721. A digital game by the name of "CryptoKitties" introduced this new standard of non-fungible tokens. Before this, almost all Ethereum tokens followed the ERC-20 protocol which meant that tokens were fungible (Valeonti 3). But how exactly are NFTs kept track of and managed? All NFTs rely on cryptography for their security. This allows the owner, or anyone intended to see the NFT to actually see the NFT while others will see a bunch of random keys. This works with the use of public and private keys. Everyone on the network has a public and a private key in which other people use your public key to encrypt a message for you. In order for you to view the message or the file, you must enter your private key which then causes the network to decrypt the message allowing you to view it (Anderson 7). Each NFT has a specific tokenId also called a uint256 variable. This is the reason why no NFT are the same as they could look exactly alike but no matter what the tokenId would differentiate them. This allows people to verify who owns what NFT as well. Basically, to prove ownership of the NFT, you have to show that you have the original hex values of the NFT (Wang 5).

Drawbacks of NFTs

NFTs have plenty of drawbacks as well. To name a few, NFTs can be tampered with, can be spoofed and many more. Most of the NFT data is stored in the blockchain. With some of the data not being stored on there, it can allow for malicious nodes to tamper with the NFT. NFTs are also liable to spoofing. This is where another person manages to get the private key or exploit ay verification methods of the NFT allowing them to transfer the NFT (Wang 9). It can also be where a attacker is able to mint/create a counterfeit NFT and give it an address of someone important raising the value (Guidi 4).

Conclusion

Blockchain, cryptocurrency, and NFTs have a lot of hype building around them for the future. With Blockchain continuing to grow every year and improvements being made, it is sure to keep growing. This paper highlighted Blockchains' significant role in developing cryptocurrencies and NFTs. Although Blockchain faces significant challenges with scalability along with other things, it is sure to keep expanding and growing every year. This technology will continue to shape the future with decentralized finance starting to become a thing and digital ownership as well. This is the start of a journey of digital revolution that has endless possibilities for the years to come.

Bibliography

A Brief Survey of Cryptocurrency Systems | IEEE Conference ..., ieeexplore.ieee.org/document/7906988/. Accessed 4 Feb. 2024.

Ammous, Saifedean. "Blockchain Technology: What Is It Good For?" *SSRN*, 1 Sept. 2016, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2832751. Accessed 1 Feb. 2024

Anderson, Dwayne. "Non Fungible Tokens Nfts." *Google Books*, Google, 4 Nov. 2021, Non Fungible Tokens NFTs - Dwayne Anderson - Google Books

Crumpler, William, et al. "What Is Blockchain, and How Does It Work?" The Human Rights Risks and Opportunities in Blockchain, Center for Strategic and International Studies (CSIS), 2021, pp. 3–8. JSTOR, http://www.jstor.org/stable/resrep38681.5. Accessed 1 Feb. 2024.

Dekker, Brigitte, et al. "The Emergence of Decentralized Finance." The Geopolitics of Digital Financial Technologies: A Chance for Europe?, Clingendael Institute, 2022, pp. 6–7. JSTOR, http://www.jstor.org/stable/resrep40265.6. Accessed 4 Feb. 2024.

Guidi, B., Michienzi, A. Delving NFT vulnerabilities, a sleepminting prevention system. Multimed Tools Appl 82, 46065–46084 (2023). https://doi-org.unco.idm.oclc.org/10.1007/s11042-023-16087-1

Luther, William J. "Bitcoin and the Future of Digital Payments." *The Independent Review*, vol. 20, no. 3, 2016, pp. 397–404. *JSTOR*, http://www.jstor.org/stable/24562161. Accessed 1 Feb. 2024.

Murray, Michael D. "NFTs and the Art World - What's Real, and What's Not." UCLA Entertainment Law Review, 29, 2021-2022, pp. 25-58. HeinOnline, https://heinonline.org/HOL/P?h=hein.journals/uclaetrlr29&i=28. Accessed Feb. 2024

Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System." Bitcoin.org, 2008, https://bitcoin.org/bitcoin.pdf Accessed 1 Feb. 2024

Reiff, Nathan. "Bitcoin vs. Ethereum: What's the Difference?" *Investopedia*, Investopedia, www.investopedia.com/articles/investing/031416/bitcoin-vs-ethereum-driven-different-purposes.asp. Accessed 4 Feb. 2024.

Tambe, Nikita. "Advantages and Disadvantages of Cryptocurrency in 2024." *Forbes*, Forbes Magazine, 10 Jan. 2024, www.forbes.com/advisor/in/investing/cryptocurrency/advantages-of-cryptocurrency/.

Valeonti, Foteini, et al. "Crypto Collectibles, Museum Funding and OpenGLAM: Challenges, Opportunities and the Potential of Non-Fungible Tokens (NFTs)." Applied Sciences, vol. 11, no. 21, 2021, p. 9931, https://doi.org/10.3390/app11219931.

van den Berg, Willem. *Blockchain for Fragile States: The Good, the Bad and the Ugly*. Clingendael Institute, 2018. *JSTOR*, http://www.jstor.org/stable/resrep17341. Accessed 1 Feb. 2024.

Wang, Qin, et al. "Non-Fungible Token (NFT): Overview, Evaluation, Opportunities and Challenges." *arXiv.Org*, 25 Oct. 2021, https://arxiv.org/abs/2105.07447

Whitaker, Amy. "Art and Blockchain: A Primer, History, and Taxonomy of Blockchain Use Cases in the Arts." *Artivate*, vol. 8, no. 2, 2019, pp. 21–46. *JSTOR*, https://www.jstor.org/stable/10.34053/artivate.8.2.2 Accessed 1 Feb. 2024