IPEC Journal of Science & Technology, Vol. 02 (02), Dec 2023
ISSN: 2583-3286(Online)

MetaMint

Shashank Goyal, Shashwat Thakur, Shivam Kapoor,Shivanshu Manna, Dr. Ragini Karwayun
Department of Information Technology
Inderprastha Engineering College, Ghaziabad, India

Abstract: **Blockchain technology is a modernized, improved database system, the main principle of which is decentralization. Blockchain allows its participants to exchange cryptocurrency and data over secure channels. The data contained in the blockchain database are in blocks interconnected in one chain. Hence the name - Blockchain. The system is practically immune to hacking, fraud and data modification, has built-in mechanisms to prevent unauthorized entry of transactions. Anyone who tries to make changes will immediately notify the system participants about the changes. The data in the Blockchain system is divided into common blocks, which are linked to each other through unique identifiers in the form of cryptographic hash functions. In 2015, the Ethereum Blockchain was launched, the main characteristic of which was the ability to create "smart contracts". Smart contracts are permit immutable trusted transparent transactions, an agreement between one or a group of parties which completely eliminate the need for a central or auditing authority. Thanks to smart contracts it became possible for application developers to create decentralized applications (DApps), decentralized finance(DeFi) and NFT applications. Like any other computer code that requires CPU resources for its execution, smart contracts consume gas instead. Gas is a Blockchain transaction fee which is paid to network validators in past miners for their work on the Ethereum Blockchain. In other words this is a cost required for a transaction to be added to the Ethereum network. The gas cost is based on many factors, that we may influence. One of the factors we can influence is writing optimized smart contracts. This study aims focuses on all possible ways to reduce gas during Ethereum blockchain transactions with a focus on mint and NFT transfer .An analysis will be made of what affects the cost of smart contracts, technologies that allow NFT creators to mint their work of arts without spending any gas fees. This study will analyse the contract ERC721a, which allows minting an entire collection of NFTs paying as for a mint of one piece. At the end we will analyse the prototype of creating an NFT marketplace with an optimized cost of gas transactions for minting and transferring NFTs and tools that were used for this implementation.**

Keywords **- Web 3.0, NFTs, MetaMask, Smart Contract.**

.

I. INTRODUCTION

Nowadays, users increasingly use and adopt technologies like artificial intelligence, virtual reality, the internet of things, etc. Another new technology called blockchain appeared a few years ago and is being adopted by many users and organizations to jump to the following internet era, the decentralization era. From the emergence of the first blockchain to the present day, many other blockchains have seemed to improve the first one. One of the most valuable improvements is the possibility of creating new applications on it. Creating applications on a blockchain is the main topic to discuss. Still, firstly, to better understand how to develop these applications, it is necessary to go deeper on a blockchain basis and know its main features. In this work, the smart contracts and some blockchains that use them to add some blockchain functionalities are also presented theoretically. After it, decentralized applications and their main components are explained, followed by the new generation of web pages born from the union of technologies discussed before. The last theoretical topic are non-fungible tokens (NFTs). This section introduces this new technology, its properties, and future applications. The concepts discussed before are put together in a practical case that shows how these different technologies work and bring a new and disruptive point of view about the internet. This work is for those who want to learn more about this technology. Some parts are very technical, so some programming or computer science concepts are necessary to understand completely. The main goal of this work is to develop a decentralized application (DApp) able to create and manage NFTs in order to provide some benefits to the holders. This DApp is programmed to run on whichever EVM-compatible blockchains. The application demonstrates that whichever business can take advantage of NFTs and generate benefits for both the company itself and the customer.

II. RESEARCH METHODOLOGY

A. Blockchain-

- Fourteen years ago, between 2008 and 2009, the

Date of Submission: 13 Nov 2023
Date of Acceptance : 25 Dec 2023
Corresponding Author: Dr. Ragini Karwayun
(e-mail: ragini.karwayun@ipec.org.in

first cryptocurrency appeared in our world in the middle of an economic crisis, and new technology came with it. This technology is called blockchain, and the reason is that in this kind of data structure, the transactions are stored in blocks. After filling a block with transactions, a new one is created, and this new block is connected to its previous one throughout the parent block hash number, thus forming a blockchain. Each block is mined from time to time, and this time is different in each blockchain. The time that needs a block to be mined is known as block time. (Haynes 2022.)

- The first blockchain was called Bitcoin, like its cryptocurrency. The bitcoin blockchain is specifically created to store and manage bitcoin cryptocurrency transactions, but it is slow. For this reason, nowadays, new blockchains and different types of blockchains are appearing. Ethereum, Solana, and Monero are examples of new popular blockchains that try to improve the Bitcoin blockchain lacks. (Haynes 2022.)

- Ethereum blockchain specializes in managing smart contracts and the information stored in them. This approach is different from bitcoin because blockchain technology is well suited to handle other information beyond cryptocurrency transactions. Another interesting use case could be tracing packages or tracking the product manufacturing process. For example, when a user buys a box and the asset to be tracked reaches some stage, this information is added to the blockchain. Then, the buyer can check the package status. Due to blockchain immutability property, nobody can modify information stored on it. Therefore, the user can trust that the package is where the blockchain says. (Ditsche and Streichfuss 2021.) Currently there exists two main types of blockchains: - Public or permissionless: On these blockchains, anyone can create blocks or be a bookkeeper without needing permission from an authority. Bitcoin is an example of a public blockchain. (Seth 2021.) - Private: These blockchains are formed by verified participants, so they are not truly decentralized because the organization controls them. But the information is not stored on a central server. It is stored among distributed ledgers. Blockchains used by private organizations are examples of it. (Seth 2021.) Other types of blockchain exist, but it is unnecessary to explain because it is beyond this work's scope

B. Smart Contract-

- Some new blockchains appear to solve other blockchains' problems or improve some aspects of them. Ethereum seems to improve Bitcoin in programming aspects. In the book Mastering Ethereum: Building smart contracts and DApps,

- Antonopoulos and Wood say that “Unlike Bitcoin, which has a very limited scripting language, Ethereum is designed to be a general-purpose programmable blockchain that runs a virtual machine capable of executing code of arbitrary and unbounded complexity.”

- Due to smart contracts rising popularity, other developers began to develop their blockchain using Ethereum’s strategy, i.e., allowing the community to develop their own applications for the blockchain. This is the case of Terra or Solana, among others. (Barker 2021; Terra.) It is also possible to build an EVM-compatible blockchain, like Binance Smart Chain (BSC). This means that an independent blockchain exists from Ethereum, but the EVM engine is used to compile the smart contracts deployed on an EVM-compatible blockchain. This approach allows using smart contracts in the same way that Ethereum does. (Temitope B.)

- Furthermore, there exist blockchains that use different approaches, like Bitcoin, which is the most famous blockchain and the first one. Bitcoin blockchain doesn’t use smart contracts in this same way. It uses smart contracts to manage transactions but does not create DApps or allow developers to do it. Each blockchain has its particularities to code and deploy smart contracts

C. Decentralized Applications (DApps)-

- On many websites, decentralized applications (DApps) are defined as a smart contract with a frontend, but this definition is wrong. If a centralized company manages the smart contract and their data are also centralized, this is not a DApp. In fact, it is a traditional centralized application. A real DApp is formed by different components that must be truly decentralized to accomplish the DApp purpose. (Antonopoulos & Wood, 2019, 475.)

- A DApp is an application whose data storage, frontend, backend, message communications, and name resolution are partially or entirely decentralized. (Antonopoulos & Wood, 2019, 475.) Technically this is tricky to achieve but not impossible. Many tools to decentralize an application are being deployed due to the rising up blockchain popularity. For example, Pinata is a very nice site to store data, Ethereum Name Service allows to buy a decentralized domain name, and other tools exist to achieve the goal of creating a DApp itself.

- DApp is composed of some elements that must be decentralized in order to build a real DApp.

ISSN: 2583-3286(Online)

- These elements are: Backend: Also known as a smart contract. It is the part where the business logic is programmed, or in other words, what a DApp is able to do. The backend should be kept as light as possible because deploying a smart contract or executing a function costs gas. The larger the smart contract or function to be executed, the more expensive it will be to deploy it. The gas cost acts as a security system because, without this gas, it would be possible to execute a function that never ends, which could cause a lot of trouble to the network. Then it is necessary to pay a transaction cost each time a transaction that modifies the blockchain (Upload or modify blockchain data, upload smart contract, etc.) is executed. It's possible to run functions as long as the economy allows. (Antonopoulos & Wood, 2019, 477.)

- Frontend: Programming languages like HTML, CSS, or JavaScript can be used to program the graphical user interface part. It is unnecessary to have advanced knowledge about EVM because the programmer doesn't interact with it. It only uses well-known tools, libraries, and frameworks to make DApp usage user-friendly. This front-end is usually programmed with JavaScript and uses libraries like web3.js or ethers.js. These libraries help communication between the front-end and the smart contract. (Antonopoulos & Wood, 2019, 478.)

D. Web 3.0-

- Web 3.0 is a new term used to refer to the latest version of traditional webs. But another term called Web3 was coined by Dr. Gavin Wood (Ethereum founder) to refer to Web 3.0 focusing on blockchain purposes. Many web pages and writers use Web 3.0 and Web3 terms in the same way, which causes some confusion to newbies. In order to avoid this possible confusion to the reader, these two different terms are exposed in the next lines.

- Web3 is a very new topic in the blockchain world, so its information is scarce and constantly evolving. Firstly, to understand Web3 and its origins, it is necessary to explain web 1.0 and web 2.0.

- Web 1.0: Also known as static websites. This kind of webpage was the first on the internet, was used from the earlier nineteens to 2005 approximately. These websites were read-only, which means the information was written by the developers on the webpage, then the users read this information. The webpage could not be edited by users, e.g., by adding comments or creating a post. (Bhattacharya 2021.)

- Web 2.0: In the mid-2000s, an evolution of web 1.0 appeared and is still used. Now the website can be edited by users because they can add data to it. This kind of web was readable-writeable. The negative side is that once this data is on the internet, it cannot be controlled by users. Furthermore, the platform and data are centralized, which means that a hacker only needs to attack the company servers to steal data or provocate bad platform behavior. Web3 appears to solve these problems. (Bhattacharya 2021.)

- Web 3.0: Web3 is DApp's frontend allocated on a blockchain. No personal data are involved because users are registered using a crypto wallet, like Metamask, Coinbase, or another wallet allowed by the website. The process to connect a user with a Web3 website would be similar to the next one: A wallet extension is installed in the user's browser. Then, when the user wants to be registered on a new website, only the wallet must be connected to the website. This is an easy step because only a click on the webpage button to link the wallet to this website is needed. The information provided by the wallet is anonymous because, from the website point of view, only a public address (wallet public key actually) has been connected. There are no user names or emails that can be linked with a person. These data are decentralized because the DApp backend is on a blockchain. Then, nobody can control it, and companies cannot sell users' data. (Dabit 2021.)

E. NFT-

- NFTs are a very new concept and are a very disruptive technology. NFT is the acronym for Non-Fungible Token. The word "fungible" means that something exactly equal or with the same value exists. Because these tokens are non- fungible, it can be said that there are not two NFTs exactly equal, and this is the main characteristic of this new technology. Then an appropriate definition of NFT could be a type of cryptographic asset representing a unique item (Hedera.)

- NFTs was firstly launched in the Ethereum blockchain. This first project was launched in 2015 and was called Etheria. Currently, blockchains like Solana support NFTs as well. One advantage of Ethereum regarding other blockchains is the creation of standards (smart contract samples) for this type of token, which makes NFTs development tasks more manageable. But because of high fees in the Ethereum blockchain, the NFT market is moving to cheaper blockchains like Solana (White-Gomez 2021; Joshua 2021 A; Canny 2022.)

- Nowadays, some people consider NFTs a scam, which could be partially true. Once something generates money, the scammers appear to take advantage of the situation and try to scam newbies.

- Scams partially appear because some people don't know how NFTs should be bought. Purchase an NFT is not only connecting the wallet to the marketplace and acquiring it. It is about getting information about the project. Knowing the founders, their experience in NFTs, the NFT utility, and if they can keep their word and accomplish the promises. These all are essential points to check before buying an NFT. (Yang 2022.)

- Another reason why people think that NFTs are a scam is that NFTs are currently mainly used to sell digital art pieces. Although NFTs are used in other areas, such as gaming, art is where the most money is spent. In 2021, $22 billion were spent by collectors and investors in digital art. NFTs are mainly used to sell art, and historically good artwork has increased in value over time. Then, many NFTs are bought by people who hope that the NFT value will rise and makes them rich. Unfortunately, this is far from reality because only a few collections are good enough to increase their value. This belief that an NFT could be worth two or three times as much in the future comes from collections like CryptoPunks. Five years ago, these collection items were gifted or sold for around $3, but now the most expensive one is "CryptoPunk 7523," which is $11.75 million worth. (Escalante-De Mattei 2021; Bureau 2021).

- Another similar case exists. In April 2021, the first NFT of a collection named "Bored Ape Yacht Club" was sold for $188 approximately. Currently, the cheapest one is around $187.000. Because of these collection growths, some people try to find the next millionairemaker collection, so when this does not happen and NFT turns cheaper or loses value, the users feel scammed. Thinking that most NFT collections will increment their value is wrong. According to Gary Vaynerchuk, entrepreneur and NFT investor, most NFTs will be worthless in a few years, and only a few collections will increase their value. (NonFungible 2022; Rosen 2022.)

- NFTs can also be used in businesses, and the main reason is, again, digital ownership. There already exists NFTs collections that provide some benefits to the holders. These benefits are not monetary, but the holders have access to exclusive events, restaurants, and courses. And this is the main utility of NFTs, providing benefits to communities.

III. CONCLUSION

Currently, there still exists a lot of ignorance about blockchain, DApps, smart contracts, NFTs, and all these terms. Some people think that blockchain only manages cryptocurrencies, and NFTs are only used to speculate with digital art. Maybe this is because there are only reported cases of people turning rich or poor in a few days or a few

hours in traditional media. This traditional media does not inform society about the powerful technology that supports cryptocurrencies and NFTs. They do not inform about the benefits of using this technology in a business or daily life. They only publish about extreme cases where money is involved. This is what only matters, the money. Only those curious, and maybe slightly visionaries, who do not consider these traditional media and get information from books or other specialized fonts, understand this technology and know its real power. It is essential to avoid biased media and get information from legitimate sources. Then, once the topic is understood, it is suitable to judge if it is interesting or not. For sure current blockchains have defects. There is a lot of work to do in order to improve this technology and simplify the way to use it, and this is my recommendation. Simplifying how a user creates a wallet, buys cryptocurrencies, and uses them on Web3 websites is necessary and will help expand its use. Also, educate the people to make that these people understand the technology and the tools to interact with web3. The final goal of this work was to demonstrate that this technology goes beyond the current applications and it is well suited to create new and different approaches to managing a company or other kinds of organizations. This task has been accomplished by programming a DApp that could be used in business and giving examples about new companies that use this technology differently. The importance of the use case presented in this work is the philosophy acquired and the different points of view offered to manage a business and build communities.

REFERENCES

[1] A. Goel, R.Bakshi, and K. Agrawal, " Web 3.0 and Decentralized Applications", MDPI- proceeding paper

[2] M. Ali Hisseine, D. Chen * and X. Yang, "The Application of Blockchain in Social Media: A Systematic Literature Review", MDPI-proceeding paper

[3] Abhijit Thakuria ,Bidyut Bikash Boruah,"An Overview of Web 3.0 applications in Libraries", https://www.researchgate.net/publication/360034070.

[4] Hector Ugarte,"A more pragmatic Web 3.0: Linked Blockchain Data", https:// www. researchgate.net/ publication/ 3156194 65

[5] Yanto Chandra, Non-fungible token-enabled entrepreneurship: A conceptual framework, Journal of Business Venturing Insights, https://doi.org/10.1016/j.jbvi.2022.e00323.

[6] F. A. Alabdulwahhab, "Web 3.0: The Decentralized Web Blockchain networks and Protocol Innovation,", doi: 10.1109/CAIS.2018.8441990.

[7] Yen, N.Y., Zhang, C., Waluyo, A.B. et al. Social Media Services and Technologies Towards Web 3.0., https://doi.org/10.1007/s11042- 015-2461-4.

[8] Huashan Chen, Marcus Pendleton, Laurent Njilla, and Shouhuai Xu. 2020. A Survey on Ethereum Systems Security: Vulnerabilities, Attacks, and Defenses. ACM Comput. Surv. 53, 3, Article 67 (May 2021), 43 pages. https://doi.org/10.1145/3391195

[9] Lee, WM. (2019). Using the MetaMask Chrome Extension. In: Beginning Ethereum Smart Contracts Programming. Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4842-5086-0_5.

[10] GARTNER. “Blockchain Technology: What’s Ahead?” Last Visited in 16/05/2022. Dispon´ıvel em: . [

[11] GARTNER. “Hype Cycle for Blockchain 2021; More Action than Hype”. Last Visited in 16/05/2022. Dispon´ıvel em: .

[12] AL-FUQAHA, A., GUIZANI, M., MOHAMMADI, M., et al. “Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications”, IEEE Communications Surveys Tutorials, v. 17, n. 4, pp. 2347– 2376, Fourthquarter 2015. ISSN: 1553-877X. doi: 10.1109/COMST.2015. 2444095.

[13] CHETTRI, L., BERA, R. “A Comprehensive Survey on Internet of Things (IoT) Toward 5G Wireless Systems”, IEEE Internet of Things Journal, v. 7, n. 1, pp. 16–32, 2020. doi: 10.1109/JIOT.2019.2948888.

[14] ALRASHDI, I., ALQAZZAZ, A., ALOUFI, E., et al. “AD-IoT: Anomaly Detection of IoT Cyberattacks in Smart City Using Machine Learning”. In: 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), pp. 0305–0310, 2019. doi: 10.1109/CCWC.2019. 8666450.

[15] SUN, J., YAN, J., ZHANG, K. Z. K. “Blockchain-based sharing services: What blockchain technology can contribute to smart cities”, Financial Innovation, v. 2, n. 1, pp. 26, Dec 2016. ISSN: 2199-4730. doi: 10.1186/s40854-016-0040-y.