A Green NFT Approach for Decentralized Proof of Ownership in Asset Management

1st Vaishali Hirlekar
Computer Engineering Department
Shah and Anchor Kutchhi Engineering College,
Mumbai, India

2nd Rohit Sinha
Computer Engineering Department
Shah and Anchor Kutchhi Engineering College,
Mumbai, India

3rd Ananya Tripathi
Computer Engineering Department
Shah and Anchor Kutchhi Engineering College,
Mumbai, India

4th Husain Lokhandwala
Computer Engineering Department
Shah and Anchor Kutchhi Engineering College,
Mumbai, India

***Abstract*—The rapid increase in fraudulent reproduction and misuse of digital certificates has become a critical concern for organizations and institutions worldwide. Fake or tampered certificates are often used to obtain employment in domains where individuals lack the required qualifications, thereby compromising organizational credibility and posing significant risks, particularly in sensitive sectors such as healthcare. With the proliferation of online learning platforms, certificates are issued digitally, making them vulnerable to unauthorized access, duplication, and identity forgery. To address these challenges, this paper proposes a secure and sustainable framework for proof of ownership of valuable educational assets using blockchain technology. Leveraging the capabilities of non-fungible tokens (NFTs), the proposed system ensures that each certificate is uniquely identifiable, tamper-proof, and verifiable. Unlike fungible digital assets, NFTs represent immutable and distinct records on the blockchain, enabling transparent and decentralized ownership verification. The proposed approach not only enhances trust and authenticity in educational credentials but also demonstrates applicability across multiple domains, including healthcare, supply chain, and digital asset management**

***Index Terms*— Non-Fungible Tokens (NFTs), Proof of Ownership, Proof-of-Stake (PoS), Data Security, Smart Contracts.**

I. Introduction

With the growing concern for environmental sustainability, there is a pressing need for industries and individuals to adopt eco-friendly practices. The world of finance is not an exception to this trend. The recent emergence of blockchain technology and the adoption of cryptocurrencies have opened up a whole new realm of possibilities for creating sustainable financial solutions. One of these solutions is the use of Green NFTs (Non-Fungible Tokens) to prove ownership of valuable assets while promoting environmental sustainability.

Green NFTs are a form of digital asset that are unique and irreplaceable, and they are often used to represent ownership of physical assets such as real estate, artwork, and collectibles. These NFTs are created on blockchain technology, which provides a secure and transparent platform for recording and verifying transactions. Green NFTs differ from traditional NFTs in that they are specifically designed to promote environmental sustainability and reduce the carbon footprint of financial transactions.

The concept of using NFTs as a means of proving ownership of valuable assets is not new, but the introduction of green NFTs takes this concept a step further by incorporating eco-friendly practices. The idea is to create a new type of NFT that is not only unique and secure but also promotes sustainable financial practices. Green NFTs achieve this by offsetting their carbon footprint through the purchase of carbon credits, which represent a reduction in greenhouse gas emissions.

The use of green NFTs has the potential to revolutionize the way we think about ownership and sustainability. For example, imagine a world where real estate ownership is transferred through green NFTs that offset their carbon footprint. This would not only ensure a transparent and secure transfer of ownership, but it would also contribute to reducing the carbon footprint of the real estate industry. Similarly, green NFTs can be used to prove ownership of artwork and collectibles, creating a more sustainable market for these assets.

The development of green NFTs also presents an opportunity for financial institutions to incorporate sustainable practices into their operations. By adopting green NFTs, financial institutions can demonstrate their commitment to environmental sustainability while providing secure and transparent financial solutions. This could lead to a shift in the way we view financial institutions and their role in promoting sustainable development.

Another advantage of using green NFTs is that they provide an opportunity for individuals and organizations to make a positive impact on the environment. By offsetting the carbon footprint of

their transactions through the purchase of carbon credits, individuals and organizations can contribute to the reduction of greenhouse gas emissions. This not only benefits the environment but also creates a sense of social responsibility and purpose.

The fraudulent reproduction of certificates has increased considerably in recent years, creating a huge headache for many organizations. Fake certificates can be used to secure employment in fields for which an individual is not qualified, damaging the reputation of businesses and awarding bodies.There are various types of courses that are taught online and after the completion of a particular course,the certificate is sent to the account of the user. There can be cases where someone gets their hands on someone else's digital certificate and they forge their name on the certificate and market it as their own certificate.

What is Proof of Ownership in Blockchain? Blockchain technology presents the perfect solution for taking digital ownership to the next level.The ability for blockchain proof of ownership across a range of different assets is essentially thanks to the introduction of non-fungible tokens

(NFTs).Unlike fungible cryptocurrencies, non-fungible tokens (NFTs) represent unique pieces

of data on the blockchain.offering transparency, decentralization, and cryptographic security, blockchain proof of ownership applies to a range of different industries. This includes the Education, Medical, Fashion, Sports, Music, and Supply Chain Management industries.

.

II. LITERATURE SURVEY

Rami Khalil and Naranker Dulay[1] discussed about the layer-two protocols that has been highlighted in order to increase the throughput of permissionless blockchains by enabling parties to lock funds into smart-contracts and perform payments through peer-to-peer communication, only resorting to the smart contracts for protection against fraud. Current protocols have fixed periods during which participants can dispute any fraud attempts. However, current blockchains have limited transaction processing capacity, so a fixed dispute period will not always be sufficient to deter all fraudulent behaviour in an off-chain protocol. In this paper they present a novel mechanism for adaptive dispute cutoffs (ADCs) which ensure that users retain the opportunity to dispute fraudulent behaviours despite blockchain congestion, while increasing second-layer protocol efficiency by reducing dispute period lengths when the number of disputes is low. They present a non-interactive argument system for setting adaptive dispute periods under the current Ethereum Virtual Machine, and describe how to efficiently integrate built-in support for adaptive dispute periods in any blockchain using binaryindexed trees. They empirically show that ADCs are possible. Layer 2 protocols can handle more disputes. Prevents more fraud than non-compliant If the user objects for denial of service, or Blockchain overload.

Satoshi Nakamoto[2] briefed about a pure peer-to-peer version of e-money that allows you to do online Payments sent directly from one party to another party financial institution. Digital signatures are part of the solution, but most importantly The benefits are lost if you still need a trusted third party to prevent double spending. We propose how to solve the double spending problem using peer-to-peer networks. The network timestamps transactions by hashing them into a continuous chain. Hash-based proof-of-work forming records that cannot be changed without iteration proof of work. The longest chain is The event has been witnessed, but it proves to have originated from the largest pool of CPU power. As As long as most CPU performance is controlled by uncooperative nodes Attacking the network creates the longest chain to overtake the attacker. of The network itself requires minimal structure. Messages are sent to the best of our knowledge and belief Bases and nodes are free to leave and rejoin the network, accepting a maximum amount of time Evidence of the work chain as proof of what happened while they were gone. They proposed a system of electronic commerce that does not rely on trust. they started with A normal framework for coins from digital signatures that offers strong control Something imperfect that you own but have no way of preventing double spending. To solve this, Proposed a peer-to-peer network that uses proof-of-work to record the publication history of transactions This quickly becomes computationally impractical for attackers to modify honest nodes Controls most of CPU performance. The network is unstructured, simple and robust. node Everything works at once with very little adjustment. It doesn't have to be identified as a message. It is not directed to any specific location and must be delivered to the best of our ability. knot can Leaving and rejoining the network and accepting the proof of work chain as proof of what It happened while they were gone. They vote on CPU performance and express their approval Reject work on them by working to extend valid blocks and rejecting invalid blocks they. All necessary rules and incentives can be enforced in this consensus mechanism. Hiroki Watanabe et.al[4], have discussed about a new

mechanism used to ensure Blockchain applied to digital-like contract management rights management. This mechanism includes new consensus How To Create A Hybrid Blockchain Using Trust Scores By alternating this new method with Proof of Stake. of Can prevent attackers from monopolizing Save resources and keep your blockchain protected. They have new mechanisms to ensure security Blockchain for contract management. serious problem In contract management is that the coin price will collapse When using a proof-of-stake process, do not act as a deterrent to attacks. To solve this they developed a new consensus How to Use Confidence Scores to Explain Hybrids Blockchains created by alternating with this new method Proof of Stake. They also modeled attacks on hybrids Revealed the blockchain and its potential for completion. Topics for our future work include: Mechanism for actual implementation Cryptocurrency.

Farhan Khan et.al[5], have discussed about enhancing Non- Fungible tokens for the evolution of Blockchain technology. A non-fungible token (NFT) is a new type of token A unique, indivisible blockchain-based token. they are First announced in late 2017. NFT is a type of blockchain-based Virtual assets attracting a lot of interest from investors Short time. Since the beginning of 2021, the phenomenon and its The market has increased dramatically. blockchain revolution Brings many changes that the art world can experience Advantage of. The purpose of this white paper is to provide comprehensive information. Information about NFTs, including applications, methods, etc. Operation, purchase, creation and sale of procedures its usefulness. NFT when combined with Metaverse is Important advances and revolutions in the virtual realm Reality and Blockchain Give Artists New Ways of Expression Their unique and precious works. This study completes the concept Practical Knowledge Gaps by Demonstrating Usefulness NFT in the field of substantive development and innovation In new private and public blockchain applications. This document introduces the rapidly growing technology Known as NFTs (Non-Fungible Tokens). NFTs are unique Cryptographic assets built on blockchain (most commonly Ethereum) representing digital art A unique identification code. Although it is a new technology, NFT has built a strong market presence through hedging More than US$2.5 billion in sales in the first half of 2021 Why: Artist and art lover. Artists have a new way to uniquely display their paintings Work in the world, lovers don't have to go to strangers anymore A market to see and buy art. In this study, Relationship between virtual currency and NFT market, Add to the increase in knowledge of the latter. As State-of-the-art technology, but with major problems Forget natural art and history A preserved art form may become extinct in the future. of The future is in our hands,make wise decisions.

Wajiha Rehman et.al[6], discussed about NFT's applications and challenges. The paper explores the concept of Non-Fungible Tokens (NFTs), which are unique digital assets that are stored on a blockchain. Unlike traditional cryptocurrencies such as Bitcoin or Ethereum, which are fungible (i.e., interchangeable), NFTs are non-fungible, meaning each one is unique and has its own distinct value.The authors discuss the various applications of NFTs, including in the fields of art, gaming, music, and real estate. In the art world, NFTs have gained significant attention in recent years, with several high-profile sales of NFT-based artwork fetching millions of dollars. NFTs can also be used in gaming to represent in-game assets such as weapons, skins, or characters. In the music industry, NFTs can be used to represent ownership of a particular song or album, providing a new revenue stream for artists. In real estate, NFTs can be used to represent ownership of a particular property, providing a more secure and transparent way of transferring ownership.The paper also provides a detailed overview of the underlying technology behind NFTs, including the use of blockchain and smart contracts. The authors highlight the unique features of NFTs, such as immutability, transparency, and ownership verification, which make them ideal for use in various applications.

However, the paper also discusses several challenges associated with NFTs, including issues related to scalability, interoperability, and sustainability. As NFTs become more widely used, scalability becomes a concern due to the limited processing power of existing blockchain networks. Interoperability is also a challenge, as NFTs are currently limited to specific blockchain networks, making it difficult to transfer them across different platforms. Additionally, the environmental impact of blockchain technology, particularly the energy consumption required for mining, is a growing concern.

The paper also covers the legal and regulatory framework surrounding NFTs and their impact on intellectual property rights. The authors discuss the various legal and regulatory issues that may arise in the use of NFTs, such as copyright infringement, data protection, and consumer protection.Overall, the paper highlights the potential of NFTs to revolutionize various industries and provides a comprehensive overview of the underlying technology and challenges associated with NFTs. The authors emphasize the need for further research and development to fully realize the potential of NFTs and address the challenges associated with their use.

Zibin Zheng et.al[7], reviewed about an overview on

smart contracts: Challenges, advances and platforms. The paper provides a comprehensive review of the challenges, advances, and platforms related to smart contracts. The authors explore the basics of smart contracts and their various applications, including in finance, supply chain management, and digital identity. The paper also discusses the challenges associated with smart contracts, such as security issues, scalability, and interoperability. The authors then review the recent advances in smart contract technology, such as the development of hybrid blockchains and new consensus algorithms. Finally, the paper examines various smart contract platforms, including Ethereum, Hyperledger Fabric, and Corda, and provides a comparison of their features and limitations. The authors conclude that while smart contracts have significant potential for revolutionizing various industries, there is a need for further research and development to address the challenges and fully realize their potential.

Sarah Bouraga[8] briefs about the Popularity of Non-Fungible Tokens: Preliminary Results. The paper examines the popularity of Non-Fungible Tokens (NFTs) in the digital market. The paper provides an overview of the NFT market and its historical growth, with a focus on the most popular NFT marketplaces, such as OpenSea and Rarible. The author analyzes the data from these marketplaces and identifies the most common categories of NFTs, such as art, gaming, and collectibles. The paper also investigates the factors that contribute to the popularity of NFTs, such as celebrity endorsements, social media trends, and viral marketing. The author concludes that while the popularity of NFTs has led to significant growth in the market, there is a need for further research to understand the long-term sustainability of this trend and its impact on the broader digital economy.

Andrew Park and Jan Kietzmann[9] discuss about The Evolution of Nonfungible Tokens: Complexity and Novelty of NFT Use-Cases. The paper explores the complexity and novelty of Non-Fungible Token (NFT) use cases. The authors analyze the historical development of NFTs and their evolution from digital collectibles to more complex use cases, such as the tokenization of real-world assets and the creation of decentralized autonomous organizations. The paper provides an overview of the different types of NFT use cases, including art, gaming, music, and sports, and identifies the factors that contribute to their success, such as network effects and community engagement. The authors conclude that NFTs have significant potential for disrupting various industries, but their success depends on addressing the challenges of scalability, interoperability, and environmental sustainability.

The research paper "Ethereum's Internet of Blockchains"[10] explores the concept of connecting multiple blockchains through the Ethereum network. The paper discusses the limitations of current blockchain technology, such as scalability and interoperability, and proposes a solution that utilizes the Ethereum network as a bridge between different blockchains. The authors describe how this "Internet of Blockchains" could enable seamless cross-chain transactions and facilitate the development of decentralized applications that operate across multiple blockchains. The paper also discusses the technical challenges associated with implementing such a system, such as managing the flow of data and ensuring consensus across multiple chains. The authors conclude that the Internet of Blockchains has significant potential for unlocking the full potential of decentralized applications and creating a more robust and interconnected blockchain ecosystem.

Nayana N. Kumar et.al[11], discussed about Decentralized Storage Of Educational Assets Using NFTs And Blockchain Technology.In the paper we see that they propose a system for securely storing and sharing educational assets using Non-Fungible Tokens (NFTs) and blockchain technology. The paper discusses the limitations of traditional centralized systems for managing educational assets, such as the risk of data breaches and lack of transparency. The authors propose a decentralized system that utilizes NFTs to represent educational assets and blockchain technology to ensure secure storage and sharing. The paper also discusses the technical details of the proposed system, including the use of smart contracts and IPFS (InterPlanetary File System) for decentralized storage. The authors conclude that their system has significant potential for improving the security and accessibility of educational assets while ensuring the privacy and ownership of the data. Sara Rouhani And Ralph Deters[12] discuss about Security, Performance, and Applications of Smart Contracts: A Systematic Survey. The paper provides a comprehensive overview of the security, performance, and applications of smart contracts. The paper discusses the advantages and limitations of smart contracts, including their potential for automating business processes, reducing costs, and increasing transparency. The authors also identify the main security threats associated with smart contracts, such as code vulnerabilities and attacks on the blockchain network, and propose various solutions to address these threats. The paper also discusses the performance of smart contracts, including their scalability and efficiency, and identifies the technical challenges associated with improving performance. Finally, the authors provide an overview of the current and

potential applications of smart contracts, including finance, supply chain management, and voting systems. The paper concludes that smart contracts have significant potential for transforming various industries but also require careful consideration of security, performance, and legal issues.

Shafaq Naheed Khan et.al[13], discuss about Blockchain smart contracts: Applications, challenges, and future trends. The paper provides an in-depth analysis of the applications, challenges, and future trends of blockchain smart contracts. The paper discusses the potential advantages of blockchain smart contracts, such as automation of processes, elimination of intermediaries, and improved transparency. The authors also identify the main challenges associated with smart contracts, such as code vulnerabilities, legal and regulatory issues, and scalability limitations. The paper also explores the potential future trends in the development and implementation of blockchain smart contracts, such as the integration of Artificial Intelligence and the use of hybrid blockchain models. The authors conclude that smart contracts have significant potential for transforming various industries but also require careful consideration of security, performance, and legal issues.

Reza M. Parizi et.al[14], discussed about Empirical Vulnerability Analysis of Automated Smart Contracts Security Testing on Blockchains.The paper presents an empirical analysis of automated security testing of smart contracts on blockchains. The paper discusses the limitations of traditional manual security testing methods and the potential benefits of automated security testing tools. The authors conduct experiments on three popular blockchain platforms (Ethereum, EOS, and Hyperledger Fabric) using various automated security testing tools to identify vulnerabilities in smart contracts. The results of the experiments show that automated security testing tools can effectively identify vulnerabilities in smart contracts and that different tools have varying levels of effectiveness depending on the platform being used. The paper concludes that automated security testing tools have significant potential for improving the security of smart contracts on blockchains and that further research is needed to improve the accuracy and effectiveness of these tools.

Dian Ross,Edmond Cretu and Victoria Lemieux[15] discuss about NFTs: Tulip Mania or Digital Renaissance? The paper provides an in-depth analysis of the phenomenon of non-fungible tokens (NFTs) and their potential impact on the art world and beyond. The paper discusses the history of NFTs, their technical characteristics, and their current and potential future applications. The authors explore the controversies surrounding NFTs, including concerns over their environmental impact and potential for market manipulation. They also examine the potential benefits of NFTs, such as providing new revenue streams for artists and enabling new forms of digital ownership and authentication. The paper concludes that NFTs have the potential to transform various industries but also require careful consideration of their social, economic, and environmental implications.

Tianyu Sun and Wensheng Yu[16] discuss about A Formal Verification Framework for Security Issues of Blockchain Smart Contracts. The paper proposes a formal verification framework for identifying and addressing security issues in blockchain smart contracts. The paper discusses the limitations of traditional testing methods for smart contracts and the need for formal verification to ensure their security. The authors present a formal verification framework that combines static analysis and runtime monitoring to detect and prevent security issues in smart contracts. They demonstrate the effectiveness of their framework by applying it to several real-world smart contracts and comparing the results with those obtained by traditional testing methods. The paper concludes that formal verification is a promising approach for addressing security issues in smart contracts and that their framework can significantly improve the security of blockchain-based applications.

Maher Alharby and Aad van Moorsel[17] discussed about Blockchain-based Smart Contracts: A Systematic Mapping Study. The paper provides a comprehensive overview of the existing literature on blockchain-based smart contracts. The paper presents a systematic mapping study that analyzes the research trends, challenges, and applications of smart contracts on blockchain. The authors review 100 papers and categorize them based on their research objectives, blockchain platforms, and application domains. They also identify the key challenges facing smart contracts, such as scalability, security, and privacy, and propose future research directions to address these challenges. The paper provides valuable insights into the current state of research on blockchain-based smart contracts and can serve as a useful guide for researchers and practitioners working in this area. Nir Chemaya and Dingyue Liu[18] discuss about Cost of Security of Layer 2 Network, Evidence from Polygon Network. The paper investigates the cost of security in the context of layer 2 scaling solutions on the Polygon network. The paper presents a detailed analysis of the economics of layer 2 solutions and examines the trade-offs between security and cost. The authors provide evidence that suggests that the cost of security for

layer 2 networks is significantly lower than that of layer 1 networks. They also analyze the effects of different security measures, such as slashing and collateral requirements, on the security and cost of layer 2 networks. The paper's findings provide valuable insights into the economics of layer 2 scaling solutions and can help inform the design of more secure and cost-effective layer 2 networks.

III. PROBLEM STATEMENT

In the digital era, the rapid transition from physical to digital assets has introduced significant challenges in ensuring authenticity, integrity, and ownership verification. Digital assets such as certificates, licenses, and legal documents are highly susceptible to forgery, duplication, and unauthorized modification due to the absence of a robust and universally accepted proof of ownership mechanism. This vulnerability facilitates illicit practices across multiple sectors, including education, healthcare, finance, and governance, where forged credentials can lead to unqualified individuals gaining access to critical roles, thereby compromising trust and public safety.

Simultaneously, traditional paper-based documents are prone to physical damage, loss, and tampering, making long-term storage and reliable verification difficult. The lack of secure, tamper-proof systems for managing both digital and physical documents creates a major barrier in establishing trust, transparency, and accountability. Existing centralized verification systems are often inefficient, susceptible to data breaches, and dependent on intermediaries, further complicating the validation process. Therefore, there is a critical need for a secure, decentralized, and immutable framework that ensures reliable proof of ownership for valuable assets, minimizing fraud while enabling efficient verification and long-term preservation.

IV. SYSTEM ARCHITECTURE

The proposed system shown in fig. 1 shows the process initiates with accessing the university's web platform, where the administrator determines the number of Non-Fungible Tokens (NFTs) to be minted in a single instance. These NFTs represent educational assets such as certificates, transcripts, or other academic credentials.

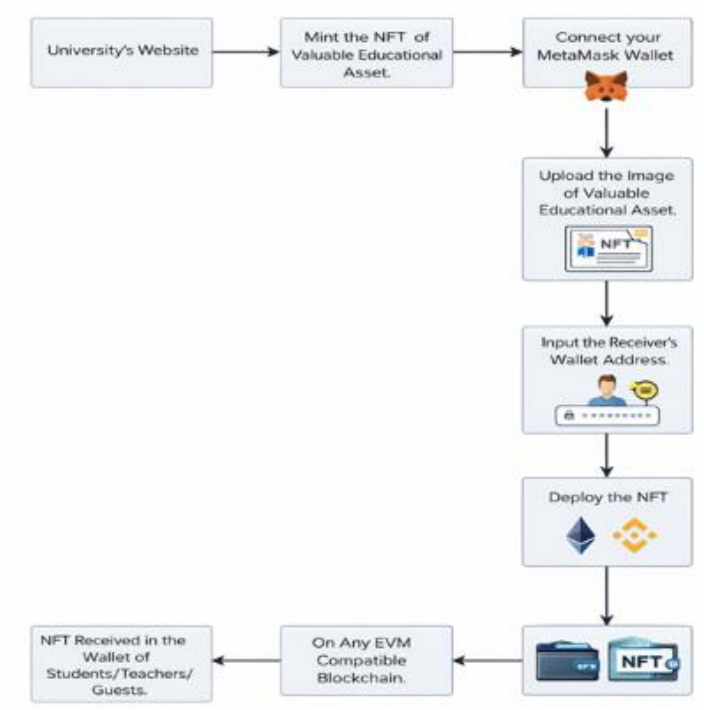

Fig. 1 Architecture for NFT-Based Educational Asset Management System

The system provides flexibility to mint either a single NFT or multiple NFTs in bulk, depending on the requirement.Both students and the university are required to connect their digital wallets, such as MetaMask, to the platform to enable secure blockchain transactions. The administrator uploads the digital asset (e.g., certificate image) intended for NFT creation and specifies the recipient's wallet address. Upon completion of these steps, the system deploys the NFT onto an Ethereum Virtual Machine (EVM)-compatible blockchain network. Once deployed, the NFT is securely transferred to the recipient's wallet address, ensuring authenticity, immutability, and verifiable ownership of the educational asset.

V. IMPLEMENTATION DETAILS

The system supports connectivity with blockchain test networks (testnets) through multiple compatible digital wallets. A widely adopted approach for wallet integration is the injected method, wherein the web application automatically detects wallets installed in the user's browser or system environment. This method scans for available wallet providers and establishes a connection seamlessly, enhancing usability and reducing manual configuration efforts.

The injected method is commonly used due to its simplicity and efficiency in connecting wallets to blockchain testnets. Once connected, users can interact with the testnet environment and perform transactions using simulated cryptocurrencies, thereby eliminating financial risks. Testnets provide a secure and controlled platform for developers and users to experiment, validate smart contracts, and test decentralized applications prior to deployment on the main network (mainnet).

Several widely used wallets support testnet connectivity, including MetaMask, Trust Wallet, and MyEtherWallet. Upon selecting a wallet, users are prompted to authenticate themselves using credentials such as passwords or passphrases. This authentication step ensures secure access and prevents unauthorized usage.

It is essential for users to safeguard their authentication credentials and avoid sharing sensitive information. Utilizing testnets not only facilitates safe experimentation but also helps prevent costly errors and unintended financial losses. Overall, integrating wallets with testnets provides a reliable and risk-free environment for developing, testing, and understanding blockchain-based systems.

A. NFT Minting and Transfer Process

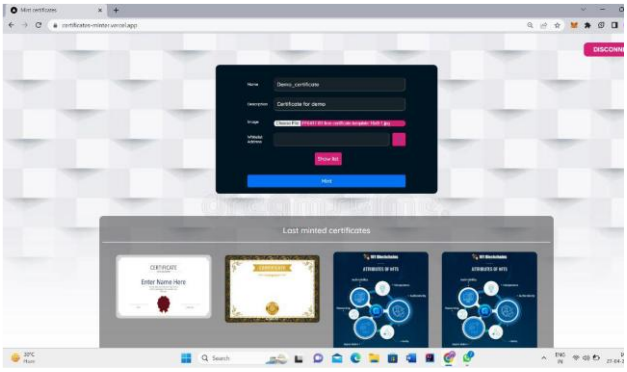

Fig. 2 shows NFT Minting process

Once the user successfully authenticates their wallet, the web interface of the proposed system is displayed. This interface provides all necessary functionalities for minting and transferring Non-Fungible Tokens (NFTs). Additionally, it maintains a record of previously minted NFTs associated with the user's wallet. Fig. 2 illustrates the NFT minting process.

After connecting the wallet to the blockchain testnet, users can initiate the certificate minting process by entering the required certificate details and uploading the certificate image in *.png* format. Upon clicking the *Mint* button, a smart contract is invoked to create the NFT on the blockchain. This process generates a unique, immutable digital asset, ensuring authenticity, ownership verification, and protection against tampering or duplication.

During the minting process, users are required to pay transaction (gas) fees, which are necessary for executing operations on the blockchain network. These fees are typically paid using cryptocurrency such as Polygon (MATIC). The gas fee varies depending on network congestion and transaction complexity. Therefore, users must ensure sufficient balance in their wallet before initiating the minting process.

Once an NFT certificate is minted, it can be transferred to another user by selecting the certificate and entering the recipient's wallet address. This action creates a new blockchain transaction, which again incurs gas fees. After confirmation, ownership of the NFT is transferred to the recipient's wallet, and the asset is no longer visible in the sender's wallet. The blockchain records this transaction permanently, ensuring transparency and traceability of ownership.

B. NFT Tracking and Verification

Platforms such as OpenSea provide a testnet environment where users can view and manage their NFTs without using real assets. By connecting their wallet, users can access the "My Items" section to monitor minted NFTs and track transaction history, including transfers and ownership changes. This functionality enhances transparency and enables verification of NFT provenance.

C. Whitelisting Mechanism

To ensure secure and controlled operations, the system incorporates a whitelist mechanism. A whitelist consists of approved wallet addresses that are granted permission to perform critical actions such as minting NFTs or transferring ownership. The whitelist is managed by an administrator, who has the authority to add or remove wallet addresses.

By restricting access through whitelisting, the system minimizes unauthorized activities and enhances overall security. Only verified users can execute sensitive operations, thereby reducing the risk of misuse or fraudulent transactions.

V. RESULTS AND DISCUSSION

The Fig. 3 shows the successful minting of a certificate as the NFT and the transfer of it to the user wallet for further use Successfully. When conducting transactions on OpenSea Testnet, users can view details such as the transaction hash, block number, gas used, and gas price. The transaction hash uniquely identifies the transaction, while the block number indicates the block in which the transaction was included. Gas used and gas price refer to the amount of computational resources consumed and the cost per unit of gas used, respectively. These transaction details are crucial for debugging and testing purposes in the development of NFT marketplaces. This page shows all the details of the NFT minting and transfer from the admin account.

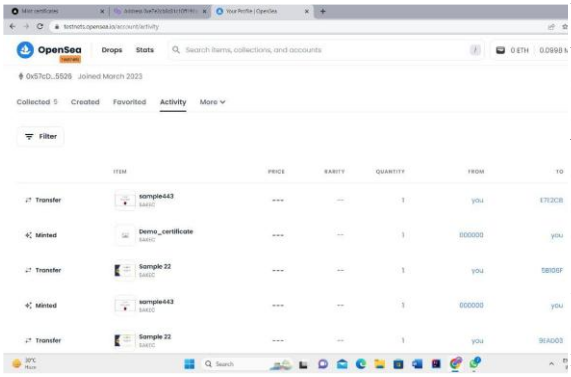

Fig. 3 OpenSea Testnet

Polygonscan is a blockchain explorer and analytics platform for the Polygon network. It is similar to Etherscan, which is a popular blockchain explorer for the Ethereum network.

Polygonscan provides users with a range of tools and features that allow them to explore the Polygon blockchain, including:

1. Block and transaction explorer: Users can explore individual blocks and transactions on the Polygon network, including information such as the sender and recipient addresses, transaction fees, gas used, and more.
2. Contract explorer: Users can view the smart contracts deployed on the Polygon network and explore their properties and functions.
3. Address explorer: Users can search for specific addresses on the Polygon network and view their transaction history, account balance, and other details.
4. Token explorer: Users can explore the tokens that are available on the Polygon network and view their price, market capitalization, trading volume, and other metrics.
5. Analytics: PolygonScan also provides a range of analytics tools, including charts and graphs that show network activity, gas usage, and other metrics.

Overall, PolygonScan is a valuable tool for developers, traders, and other users who want to explore and analyze the activity on the Polygon network. Its user-friendly interface and extensive range of features make it a popular choice for anyone looking to gain insights into the Polygon blockchain.

A. Polygon (previously known as Matic Network) is a Layer 2 scaling solution for Ethereum that aims to improve scalability, reduce fees and increase transaction speed. Here are some of the advantages of Polygon blockchain:

1. Scalability: Polygon provides a high-speed, low-cost platform that can handle thousands of transactions per second (TPS). It uses a unique architecture that allows it to process transactions in parallel, which helps to improve scalability.
2. Interoperability: Polygon is compatible with Ethereum, which means that any Ethereum-based application can easily be migrated to the Polygon network. It also supports interoperability with other blockchains, making it easy to exchange assets between different networks.
3. Low Transaction Fees: Polygon offers low transaction fees compared to Ethereum, which can be prohibitively expensive at times. This makes it easier for small and medium-sized businesses to use blockchain technology.
4. Decentralization: Polygon is a decentralized network that is governed by a community of developers and validators. This ensures that the network is transparent, secure, and free from central control.
5. Security: Polygon uses a Proof of Stake (PoS) consensus mechanism, which makes it more secure than traditional Proof of Work (PoW) blockchains. PoS ensures that validators are incentivized to act honestly, as any malicious behavior could result in the loss of their stake.
6. Developer-friendly: Polygon provides a range of tools and resources for developers, making it easy to build and deploy decentralized applications (dApps) on the network. This includes easy integration with popular programming languages such as Solidity, JavaScript, and Python.

Overall, the Polygon blockchain offers a range of benefits that make it an attractive platform for developers and businesses looking to leverage blockchain technology.

VI. CONCLUSION

This paper is an innovative solution that addresses two important concerns: the need for secure and transparent ownership of valuable assets and the urgency of promoting sustainable practices in finance. The project achieves this by using blockchain technology, smart contract coded on Solidity, and hosting the website on

Vercet, which ensures transparency, security, and sustainability in the transfer of ownership of assets.

The use of Green NFTs as a means of proving ownership of valuable assets promotes sustainable practices in finance by offsetting their carbon footprint through the purchase of carbon credits. This ensures that every transaction made through the Green NFTs has a net zero carbon impact, thereby reducing the carbon footprint of the financial industry. Moreover, the transparency and security of blockchain technology, combined with the smart contract coded on Solidity, guarantee the integrity of every transaction made using Green NFTs.

The website hosted on Vercet provides a user-friendly platform for creating, buying, and selling Green NFTs, making it accessible to a wide range of users. The website also provides detailed information on the carbon footprint of each transaction made using Green NFTs, giving users a clear understanding of the environmental impact of their actions. This transparency encourages users to take responsibility for their environmental impact and make sustainable choices in their financial transactions.

By providing a secure and transparent platform for recording and verifying transactions, it creates a more sustainable and socially responsible financial system. Moreover, the paper presents an opportunity for financial institutions to demonstrate their commitment to environmental sustainability and social responsibility, thereby enhancing their reputation and credibility.

REFERENCES

[1] R. Khalil and N. Dulay, "Adaptive layer-two dispute cutoffs on smart-contract blockchains," in Proc. 3rd Conf. Blockchain Research and Applications for Innovative Networks and Services (BRAINS), 2021.

[2] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.

[3] M. Duguleana and F. Gibacia, "Augmented reality meets non-fungible tokens: Insights towards preserving property rights," in Proc. IEEE Int. Symp. Mixed and Augmented Reality Adjunct (ISMAR-Adjunct), 2021.

[4] H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu, and J. Kishigami, "Blockchain contract: Securing a blockchain applied to smart contracts," in Proc. IEEE Int. Conf. Consumer Electronics (ICCE), 2016.

[5] F. Khan, R. Kothari, M. Patel, and N. Banoth, "Enhancing non-fungible tokens for the evolution of blockchain technology," in Proc. Int. Conf. Sustainable Computing and Data Communication Systems (ICSCDS), 2022.

[6] W. Rehman, H. Zainab, J. Imran, and N. Z. Bawany, "NFTs: Applications and challenges."

[7] Z. Zheng, S. Xie, H.-N. Dai, W. Chen, X. Chen, J. Weng, and M. Imran, "An overview on smart contracts: Challenges, advances and platforms," Future Generation Computer Systems, vol. 105, pp. 475–491, 2020.

[8] S. Bouraga, "On the popularity of non-fungible tokens: Preliminary results," in Proc. 3rd Conf. Blockchain Research and Applications for Innovative Networks and Services (BRAINS), 2021.

[9] A. Park and J. Kietzmann, "The evolution of non-fungible tokens: Complexity and novelty of NFT use-cases."

[10] "Ethereum's Internet of Blockchains."

[11] N. N. Kumar, R. R. Basale, S. Kumar, and M. Saffath, "Decentralized storage of educational assets using NFTs and blockchain technology," in Proc. 4th Int. Conf. Smart Systems and Inventive Technology (ICSSIT), 2022.

[12] S. Rouhani and R. Deters, "Security, performance, and applications of smart contracts: A systematic survey," IEEE Access, 2019.

[13] S. N. Khan, F. Loukil, C. Ghedira-Guegan, E. Benkhelifa, and A. Bani-Hani, "Blockchain smart contracts: Applications, challenges, and future trends," Peer-to-Peer Networking and Applications, vol. 14, pp. 2901–2925, 2021.

[14] R. M. Parizi, A. Dehghantanha, K.-K. R. Choo, and A. Singh, "Empirical vulnerability analysis of automated smart contracts security testing on blockchains."

[15] D. Ross, E. Cretu, and V. Lemieux, "NFTs: Tulip mania or digital renaissance?" in Proc. IEEE Int. Conf. Big Data, 2021.

[16] T. Sun and W. Yu, "A formal verification framework for security issues of blockchain smart contracts."

[17] M. Alharby and A. van Moorsel, "Blockchain-based smart contracts: A systematic mapping study."

[18] N. Chemaya and D. Liu, "Cost of security of layer 2 network: Evidence from Polygon network."