Blockchain-Based Transferable Digital Rights of Land

[1st]Ras Dwiwedi
Computer Science and Engineering
Indian Institute of Technology
Kanpur

[2nd] Sumit Patel
Computer Science and Engineering
Indian Institute of Technology
Kanpur

[3rd]Prof. Sandeep Shukla
Computer Science and Engineering
Indian Institute of Technology
Kanpur

Abstract *Land is a vital resource for any country's economic endeavors, playing a pivotal role in economic production. As such, the stewardship of land resources is viewed as a crucial part of a nation's economic policies. However, managing land in urban areas is a complex issue due to the scarcity of land and the divergent interests of multiple stakeholders. Urban local bodies are perpetually aiming to create more commercial spaces to augment their revenue. In contrast, planning authorities are pushing for stringent regulations to promote sustainable development, and development authorities require land for infrastructure projects. The city's disadvantaged residents are continually striving to regularize their tenancy. Formulating land governance policies in urban areas accommodating all stakeholders is a formidable challenge for any country. In this paper, we delve into the concept of representing land as a Non-Fungible Token (NFT) on a permissioned blockchain, which could potentially enable the trading of land as an asset. Tokenizing land could also improve liquidity, as it would permit individuals to purchase smaller plots of land instead of large areas. Integrating land into the blockchain could also help mitigate fraud and enhance efficiency among the various departments involved in the land transaction process.*

Keywords Non-Fungible tokens, Blockchain, Smart contract, Distributed Ledger, Digital Art, Provenance, Tokenomics

1 Introduction

Land, being a valuable asset, is typically held for the long term and is highly sought after for its development potential. Rapid urbanization in densely populated areas has led to a shortage of land, particularly in older parts of cities. The scarcity of land in these central areas poses a significant challenge for development authorities in creating new parks, widening roads, and implementing other infrastructure projects. However, due to their prime location, these lands carry substantial value, and owners are often reluctant to part with even the smallest portions. While it is possible to acquire land through legal means, the high compensation costs associated with it, combined with financial constraints faced by development authorities, make it impractical to acquire large amounts of land.

Transferable Development Rights (TDRs) present a mechanism that attempts to address both aspects of this problem. By decoupling the physical land from its development potential, TDRs allow the conversion of development potential into a digital tradable asset, akin to corporate shares. Unlike shares, TDR holders possess rights solely for development purposes and do not have ownership rights over the physical land.

The conversion of development potential into transferable development rights also offers a solution to the financial challenges faced by development authorities. Compensation for land can be provided in terms of TDRs instead of monetary value. This allows development authorities to acquire land without burdening their balance sheets.

This paper proposes the tokenization of TDRs on the blockchain. We argue that through tokenization and fair, transparent trading on the blockchain, users can obtain the fair market value of the land. Moreover, we contend that digitized development rights are well-suited for tokenization as they represent fully digital assets, backed by the guarantees of the development authority. To support our claims, we examine various cases of asset tokenization, where physical assets were tokenized using non-fungible tokens (NFTs). However,

we note that the linkages between the physical asset and the digital token are often weak and pose significant challenges in the tokenization process. In our implementation, TDRs represent rights backed by development authorities and are not directly linked to any physical asset until their utilization. We model the entire life cycle of TDRs, from generation and transfer to their utilization, on the blockchain. Our ultimate goal is to create a marketplace for TDRs on the blockchain, facilitating efficient and transparent land development finance. This paper is organized as follows: First we present the background on the blockchain and the asset tokenization highlighting why the linkages between the digital token and the physical asset is the problem. Then we present the TDR and its lifecycle. We then present the architecture of the out implementation.

2 Problem statement

The urban planning and development sector faces considerable hurdles in the efficient allocation, transaction, and administration of Development Rights Certificates (DRCs). Existing systems, typically manual and centralized, suffer from a lack of transparency, often leading to potential disputes and fraudulent activities. For instance, transactions such as compromise decrees, government grants, and instruments of partition are not mandated to be registered, leading to a situation where not all transactions that establish land rights are documented in the registry. Additionally, the registry fails to track land transfers occurring through inheritance. A significant shortcoming of the present land registration system, particularly the deed registration, is its inability to maintain parcel-wise ownership records. This limitation complicates the process of validating land ownership, further undermining trust and efficiency in the system. Adding to the complexity, India employs two separate subsystems for maintaining ownership records under the land registration system. These subsystems, managed by different entities, contribute to instances of fraud and inconsistencies in land information. The potential for officials to misuse their powers or perform inefficiently adds another layer of risk. These issues lead to increased processing time for public applications and a lack of transparency in procedures.The lack of transparency and completeness in record-keeping, compounded by bureaucratic inefficiencies, burdensome paperwork, and limited market access, creates considerable barriers for the swift and cost-effective transaction of land in form of DRCs. Also with the current system it is not possible to find a buyer for DRCs of bigger land areas, this causes a serious problem of liquidity in the market. By enabling DRCs in the form of blockchain NFTs, we can sell fractional ownership for a part of DRC , which is not possible with current land registration systems.

3 System Architecture

3.1 Overview of Quorum blockchain

Blockchain is a type of distributed ledger technology (DLT) designed to facilitate secure, transparent, and immutable transactions. Quorum, a variant of this technology, is a private, permissioned blockchain based on Ethereum. It enables private transactions among specific users, managing network and peer permissions to ensure that only approved nodes participate in the Quorum blockchain network.

Quorum utilizes a consensus algorithm based on voting, and it offers an Istanbul Byzantine Fault Tolerance (IBFT) consensus mechanism. As it's compatible with the Ethereum Virtual Machine (EVM), Quorum also supports smart contracts programmed in Solidity, making it a versatile and secure option for managing complex transactions and contracts within a permis-

sioned network.

3.2 NFT standard for DRCs

We have used the ERC721 protocol for issuing DRCs. ERC721 protocol, a prevalent standard on the Ethereum blockchain, is chiefly employed for non-fungible tokens (NFTs). NFTs, which are distinctive and non-divisible, are used to represent various unique digital assets such as collectibles, digital artwork, virtual real estate, and gaming items. The characteristic feature of ERC721 tokens is their distinctiveness and limited availability; each token holds a specific value and is non-interchangeable on a like-for-like basis, unlike fungible tokens.The protocol establishes a collection of functions and events that facilitate the creation, ownership, and transferability of non-fungible assets.

Our Transferable Development Rights (TDR) application, based on blockchain, is developed using the Quorum blockchain and consists of four nodes. These nodes are hosted on separate Linux servers strategically located at different sites to avoid simultaneous downtime

In our current permissioned blockchain network configuration, we've disabled "Tessera," which is Quorum blockchain's default transaction manager. We took this step because our application does not process any private transactions on the blockchain. We've also set the block mining time to five minutes, meaning that any new block that emerges will be auto-mined by the nodes.

The major components of our application include:

1) Blockchain network.
2) Quorum Transaction Signer.
3) HashiCorp Vault.
4) Backend Infrastructure.
5) Smart contracts.

The Quorum Transaction Signer has been constructed as an independent service that retrieves a user's private key from the HashiCorp Vault. Each user's private key is stored in the vault using a reference ID, which we save in MongoDB associated with the corresponding user. To fetch the private key, we prompt the user to enter their password, while the back-end server sends the reference ID. Using the reference ID, the encrypted private key string is obtained and, with the real-time entry of the user's password, the private key is decrypted. Consequently, the raw transaction is signed and transmitted to the network. This methodology allows us to privately sign transactions in a separate, secure environment, thus enhancing the security of the signature process.

Our application utilizes HashiCorp Vault for the storage of two critical pieces of information: User private keys in an encrypted format. Aadhaar numbers of users in an encrypted format. When these details are secured in the vault, it generates a unique 16-digit ID for each piece of data stored. We retain this reference number in MongoDB for future retrieval of the private key or Aadhaar number as required. For a user to successfully sign up on the platform, authentication via the Aadhaar service is necessary.

If the Aadhaar number is deemed invalid, the user's sign-up attempt will be denied. Once the user provides all the required details for registration, the form is forwarded to an administrator for approval. Upon successful verification by the administrator, the user receives an email confirmation indicating successful on boarding to the platform. Each successfully signed-up user is assigned a unique ID, which is linked to the user's Aadhaar address. This ID is used whenever necessary to fetch user details or execute any transaction

Blockchain based Transferable Development Rights

related to the user's application on the portal.The requirement for a unique Aadhaar number fosters a more permissioned and exclusive user base consisting only of authenticated and genuine buyers or sellers. This approach prevents anonymous users from gaining access to our platform.Furthermore, if a user forgets their password, they are prompted to enter their Aadhaar number. Subsequently, an OTP is sent to their mobile number for authentication. The user must input this OTP to reset their password.

3.2.1 On-chain and Off-chain Data on Blockchain Based TDR application

Irrelevant details for tracking applications are stored off-chain in our system. The following user-related information is stored off-chain:

- Photos related to the user or application.
- Documents in PDF/JPG/JPEG format.
- User's phone number and email.
- User's address.

On the other hand, all the relevant details concerning the land are stored on-chain:

- TDR application details, including notice ID, timestamp, location, circle rate, and status.
- Notice details, consisting of notice ID, timestamp, location information, property information, construction details, and property ID.
- DRC details, encompassing DRC ID, available Floor Area Ratio (FAR), land count, and owner information.

All the data stored on-chain is validated and signed by the users using their public keys. For example, when applying for a TDR application, the user fills in the required details, signs the data with their public key, and publishes a transaction to the Quorum network. This transaction is then broadcasted to all the nodes in the network, ensuring that the updated state is received by all nodes.

4 Implementation

For the on-boarding process, users are required to register on the platform using their initial credentials and unique Aadhaar card number. If a user attempts to register with an existing Aadhaar number, they will be denied access. We store Aadhaar details in a separate vault, encrypted for security purposes. The corresponding ID retrieved after storing the details in the vault serves as a reference throughout the application process. Upon successful registration, an account is created on the Quorum blockchain, containing the user's respective public and private keys. The user's private keys are stored in the HashiCorp Vault within a separate, secure environment and encrypted using a specific encryption method.

Once registered, users have the option to apply for a Transferable Development Rights (TDR) application if they have received notice regarding the piece of land they own. Upon filing a TDR application, the user is assigned a unique 16-digit number, which is stored alongside its corresponding state in our TDR smart contract. This smart contract tracks and maintains the state of each TDR ID. The TDR application undergoes a verification process by various sub-departments within the development authority. If any discrepancies are found, such as mismatches between the submitted land ownership details and the authority's system, the application is rejected or sent for updates.

The blockchain is updated accordingly through the TDR smart contract, marking the status as "REJECTED." On successful verification, the TDR application status is updated as "VERIFIED" on the blockchain through the smart contract. The TDR smart contract enables the tracking of the application's progress, ensuring accountability for any unauthorized actions by officials. Signatures of users involved in

the transaction on the TDR application can be traced, holding individuals responsible if necessary. Once an application is approved by officials, the user becomes eligible to obtain their Development Rights Certificate (DRC). As the TDR application is approved on the blockchain, the user is issued their DRC in the form of an NFT (Non-Fungible Token).

The DRC NFT contains comprehensive information pertaining to the specific land it represents. Each land detail, structured in the form of a schema, is stored on the IPFS network. The unique URL or hash generated by IPFS serves as the URI, which is subsequently stored within the NFT and transferred to the user. Consequently, each NFT possesses a distinct set of land details corresponding to the specific piece of land owned by the user. Furthermore, each NFT is signed by a KDA blockchain account, thereby establishing and validating the authentic ownership of the land. This signature serves as irrefutable proof of ownership, allowing the NFT holder to demonstrate their rightful ownership of the land to any interested party. The properties associated with the piece of land owned by the user are stored within the NFT, ensuring that all relevant details are encapsulated within the token

The aforementioned details are retrieved from the DRC contract and subsequently transmitted to the KdA-Nft contract. To transfer the DRC NFT to a user, two essential pieces of information are required: the user's address, to which the NFT is being transferred, and the URI. This URI contains a unique identifier, which may be in the form of a hash or a URL, enabling the precise representation of the NFT associated with the land ownership.

4.1 Issuance and management of TDR as NFT

The KDAKanpurNFT contract is an ERC721 token contract that represents ownership of a unique item or asset on the Quorum blockchain. This contract is used to create, manage, and transfer non-fungible tokens (NFTs) for the KDA-TDR-PORTAL.

The contract inherits from the ERC721, ERC721 URIStorage, and AccessControl contracts from the OpenZeppelin library. The ERC721 contract provides the basic implementation of the ERC721 standard for non-fungible tokens. The ERC721URIStorage contract extends ERC721 by including a URI for each token, which can point to a JSON file with more information about the land. The AccessControl contract provides a system of access control for the contract, allowing certain operations to be performed only by addresses with specific roles. The contract uses the Counters library from OpenZeppelin to keep track of token IDs. Each new token that is minted is assigned a unique ID by incrementing a counter.

The KDAKanpurNFT contract has a mapping mapDRC IdToTokenId that associates each DRC ID with a token ID, and a mapping mapTokenIdToDRCId that associates each token ID with a DRC ID. These mappings allow the contract to keep track of which DRCs are associated with which tokens. The safeMint function is used to mint new tokens. This function can only be called by an address with the MINTER ROLE.

When a new token is minted, the function assigns it a unique ID, associates it with a DRC, and sets its URI. The burnDRC function is used to burn tokens. This function can only be called by an address with the DEFAULT ADMIN ROLE. When a token is burned, the function removes it from the mapDRCIdToTokenId and mapTokenIdToDRCId mappings and calls the burn

function from the ERC721 contract to burn the token. The tokenURI function is used to get the URI of a token, and the UpdateURI function is used to set the URI of a token. These functions allow the contract to manage the URIs of tokens, which can point to JSON files with more information about the tokens.

4.2 Transfer and ownership tracking of TDR as Non Fungible Token

The ownership and transfer of Transferable Development Rights (TDRs) are tracked via tokens using the ERC721 standard for non-fungible tokens (NFTs) on the Quorum blockchain. Here's how it works:

When a TDR is created, a corresponding NFT is minted. The NFT is unique and represents the TDR. The ownership of the NFT (and therefore the TDR) is assigned to the address that created the TDR. This process is typically handled by a function in the smart contract, as safeMint in the provided KDAKanpurNFT contract. The owner of an NFT is the address that currently has control over it. This is tracked on the blockchain, and the ERC721 standard provides a function ownerOf that allows anyone to query the owner of a specific NFT (and therefore the owner of the corresponding TDR).This can be used to prove ownership of development rights for that particular piece of land.

When a TDR is sold or otherwise transferred, the corresponding NFT is transferred from the seller s address to the buyer s address. This is done by calling a function like transferFrom or safeTransferFrom in the ERC721 standard.These functions update the owner of the NFT on the blockchain.Since all these operations are performed on the blockchain, they are transparent and immutable. This means that the history of ownership and transfers of a TDR can be tracked by looking at the history of the corresponding NFT. If a TDR is utilized in the receiving zone, the corresponding NFT is burned. This is done by calling a function burn in the ERC721 standard.

5 Conclusion

In conclusion, issuing Development Rights Certificates (DRCs) as Non-Fungible Tokens (NFTs) on the blockchain presents a compelling solution to the challenges faced in land registration processes. By leveraging blockchain technology, transparency and trust are enhanced, ensuring the integrity of land ownership records.

The implementation of smart contracts streamlines the TDR application process, automating tasks, and facilitating efficient verification and approval procedures. The immutability of the blockchain ensures a transparent and auditable record of the TDR application's lifecycle, tracking its progress through various stages and holding officials accountable for their actions.The inclusion of unique identifiers, such as URIs, within the NFTs guarantees the accurate representation of land details and provides indisputable proof of ownership.

This transformative approach reduces disputes, promotes trust among stakeholders, and establishes a reliable system for tracking and verifying land ownership, ultimately improving the overall integrity of the land registration process.

6 Future Work

We are currently expanding the scope of our application by developing an on-chain marketplace specifically designed for users to trade their DRCs in a permissioned environment. This marketplace aims to provide a seamless and user-friendly platform for DRC transactions. Furthermore, we are committed to optimizing

Blockchain based Transferable Development Rights

our smart contracts and conducting bench-marking exercises to enhance their performance.

By improving the efficiency and throughput of our smart contracts, we aim to increase the Transactions Per Second (TPS) for our application. This optimization process will contribute to a more robust and scalable system, enabling smoother and faster transaction processing.

References

[1] J Michael Graglia, Christopher Mellon, Blockchain and property in 2018, At the end of the beginning, MIT Press Direct, 2018.

[2] The Role of Blockchain in Documenting Land Users' Rights, The Canonical Case of Farmers in the Vernacular Land Market

[3] OpenZeppelin. (n.d.). ERC721 - OpenZeppelin Docs, https://docs.openzeppelin.com/contracts/4.x/erc721