Landcoin: A Practical Protocol for Transfer-of-Asset

Vishwas Patil(✉) and R. K. Shyamasundar

Department of Computer Science and Engineering, Indian Institute of Technology Bombay, Mumbai, India

Abstract. Blockchains ensure integrity, transparency, and immutability of transactions they process. It also guarantees the eventual inclusion of all the transactions submitted to the blockchain and records them in its ledger. Bitcoin and Litecoin are examples of time-tested, reliable public blockchains that handle only one type of transaction – send/receive money (i.e., transfer-of-value) from one user to another. Whereas, general-purpose blockchains like Ethereum provide means and methods to encapsulate transfer of not only *value* but anything fungible that can be digitally represented with the help of programs *aka* smart contracts. However, with a high-level Turing-complete programming language to write smart contracts, Ethereum encountered vulnerabilities in its contracts thus forgoing the claim of immutability. On the contrary, script-based blockchains like Bitcoin and Litecoin have withstood the test of time and hence are perceived reliable – a very important aspect while managing assets like land. In this paper, we present a *transfer-of-asset* system for land management that borrows from Litecoin protocol its script, underlying consensus, and block structure. Our resultant system is a permissioned blockchain, where only a set of pre-approved miners can append land records to the blockchain. We introduce *sidechains* that are roped in a *mainchain*. The *mainchain* stores land records, which can be queried by citizens; whereas, sidechains hold intricate details about intermediate validations performed by regulators, registrars, and notaries. The process of land management used in this paper is a typical process in the states of India. Our system can be used to manage any asset class that is finite in nature. Our approach provides transparency of transactions at a higher level and privacy to individual transactions.

Keywords: Blockchain · Land management · Privacy · Access control

1 Introduction

In countries like India, where the land records are maintained with human intervention, they are perennially marred with presumption and excessive bureaucracy – leading to malfeasance and thus into time-consuming legal disputes [16].

The work was done at the Center of Excellence for Blockchain Research, funded by Ripple UBRI.

S. Tripathy et al. (Eds.): ICISS 2021, LNCS 13146, pp. 124–141, 2021.
https://doi.org/10.1007/978-3-030-92571-0_8

Land is a precious asset that can be used as a collateral or used for many other productive purposes only if the title deeds are indisputable and are derived using a transparent process. Land litigation is a huge cost to the economy and one of the reasons of financial exclusion for a large population. In the past decade, many of the states have migrated their paper based records to digital versions [11] but with only partial success in containing the malfeasance. Several state governments (since land ownership is state's purview in the federal system of India) are exploring the blockchain approach to inherit its natural properties – integrity, transparency, and immutability; to the land records and their transactions in a land management system. Most of the implementations are based on Ethereum smart contracts and Hyperledger Fabric; where the steps of land management process are encapsulated as smart contracts (high-level software programs), which inherit the pros and cons of any high-level programming language [5]. Another limitation of such implementations is their system's state-specific scope, which may not answer queries like; what all title deeds a subject holds in India, across the states. In other words, the current approaches that we are aware of are *not scalable across the states* and also are *not interoperable*.

In this paper, we present a land management system based on Litecoin's public blockchain codebase. We add features to modify the same to suit our purpose of having a permissioned blockchain for transfer of asset while keeping the underlying skeleton of the blockchain and its stack-based purpose specific script unchanged for the most part. Our system is scalable, interoperable, and also privacy-preserving. We achieve these desirable features by segregating the data related to a land transaction into two categories: public and private. We record the public part of the land transaction data (like, who transferred a land to whom) on mainchain and the corresponding private part of the land transaction (like, at what rate the land is sold) on a sidechain that is maintained by the state to which that land belongs. The mainchain can be queried by anyone, whereas the sidechains accept attribute-based queries only from the parties that are involved in a land transaction. In our implementation, we have introduced new transaction types to Litecoin's codebase. Each type corresponds to a distinct operation in prevalent land management workflow. We introduce separate transaction types to the mainchain and sidechains. Each land transfer transaction on the mainchain traverses through the workflow on the sidechain before getting committed on mainchain. The first transaction/step on the sidechain takes an input from the mainchain and the last transaction/step on the sidechain inputs to the mainchain. In other words, when a subject intends to transfer her land to another subject, the transaction has to go through government verification/diligence process (which gets recorded on the sidechain) before being accepted by the miners on the mainchain. Our construction allows an audit trail to traverse from mainchain to sidechain and back to the mainchain without the auditor knowing the intricate details recorded on the sidechain, which only the seller, buyer and the land authorities can decrypt. Maintaining confidentiality of transaction details while keeping the transaction trail transparent is an important feature that our system provides.

2 Background and Motivation

The prevalent land management systems use databases for storage of land records and use cryptography for data protection. While confidentiality mechanisms can be enforced, these systems fall short in maintaining an immutable trail of operations performed on land records, because tuples in a database can be overwritten. Double-entry book-keeping is used in identifying discrepancies in records, however malicious records can only be traced with the help of a digital log management system, which in turn is susceptible to tampering [18]. Triple-entry book-keeping can be adopted, where each transaction is digitally signed by the subject of transaction; irrespective of the transaction being valid, erroneous or malicious – thus fixing accountability. Most of the non-blockchain implementations of land management systems fall under this triple-entry book-keeping category. However, such centralized systems lack a real-time, transparent view.

A new type of decentralized database technology (aka DLT/blockchain) appears to be a natural fit for land management system because it not only provides all of the properties of a triple-entry book-keeping approach but also offers immutability, transparency, and real-time auditability to land transactions. The transparency and auditability for all the stages in the transfer of land coupled with the inherent immutability guarantee that a blockchain provides helps solve the double-spend and prevent similar frauds prevalent during transfer of property agreements. Furthermore, blocks chained with cryptographic hashes provide a verifiable record of all the history of the transfer of land assets, as opposed to a simple database where only the current ownership status is reflected. Databases can also store transaction history but there is no guarantee that the records have not been tampered since it was appended to the logs and the trust needs to be placed onto the authorities maintaining the database for that as well.

The choice of a blockchain protocol for land management is an important design criteria because the inherent pros and cons of the protocol reflect into the system. A judicious mix of engineering tweaks need to be adopted in order to inherit the pros and mitigate the cons. In our approach, we narrowed down on the Litecoin protocol [15] due to the following criteria: i) time-tested, proven, open protocol; ii) limited set of stack-based script operations; iii) `scrypt` based proof-of-work consensus algorithm.

A general purpose blockchain like Ethereum can be used [9,12,19] but its underlying programming language may open up avenues [5,13] for serious asset loss or inconsistent states of asset ownership, which is unacceptable. Therefore, it is prudent to rely on a protocol (like Bitcoin [17] or Litecoin [15]) that is built for a specific purpose rather than using a general purpose protocol like Ethereum [20] or Hyperledger Fabric [8]. Between the Bitcoin and the Litecoin codebase, we opted for Litecoin for its reliance on `scrypt` hashing algorithm that cannot be accelerated by ASIC processors, which is the case for Bitcoin since it uses `SHA256` hashing algorithm for block mining. To make the system adaptable for current land management practices, we had to tweak the default setup of Litecoin protocol. In summary, the following are the modifications we introduced in the Litecoin protocol.

1. New transaction types for mainchain and sidechain, each corresponding to a step in the current workflow of land management.
2. Pre-approved miners, similar to validators in XRP [14], is a set of public-keys listed by the central government through a transaction on mainchain.
3. Sidechains allow states to compose their respective land management workflows as separate chain anchored in the mainchain; there are no coinbase operations on sidechains.
4. Certifying coins and mapping them to a landmass is a one time operation during the bootstrapping phase in which all the pre-mined 84 million coins are transferred to the central government and then distributed to the state governments according to their proportionate landmasses.
5. Certified user addresses and signing keys: any entity entering the system needs to have an address and corresponding signing and verification keys. Instead of generating them locally as in the case for permissionless crypto-currencies, a Trusted Third Party (TTP) is involved in verifying identities and assigning certificates with the keys being formed jointly by both parties.

3 Architecture of Landcoin Protocol

In this section we present the design aspects of our protocol followed by practical considerations while dealing with land management.

3.1 From a Transfer-of-Value to a Transfer-of-Asset System

The following two challenges come up while extending a *transfer-of-value* system (Litecoin) to a *transfer-of-asset* system (Landcoin): i) a class of asset like money, which is represented by numbers alone, is different from the class of assets like land, which has identification attributes and does not have properties like fungibility or malleability; and ii) assets like land have certain legal requirements to be adhered to before any mutation or transfer occurs. These characteristics need to be taken into consideration while constructing the *transfer-of-assets* system. We make the following four assumptions in our design: i) during the initialization phase of our system, all the 84 million coins are mapped to units of total land; ii) all stakeholders have unique identifiers – UIDs; iii) The title deeds of land are unambiguous and the assets represented therein have unique identifiers – URIs; and iv) the pre-approved miners (i.e., transaction validators) are honest and are always available.

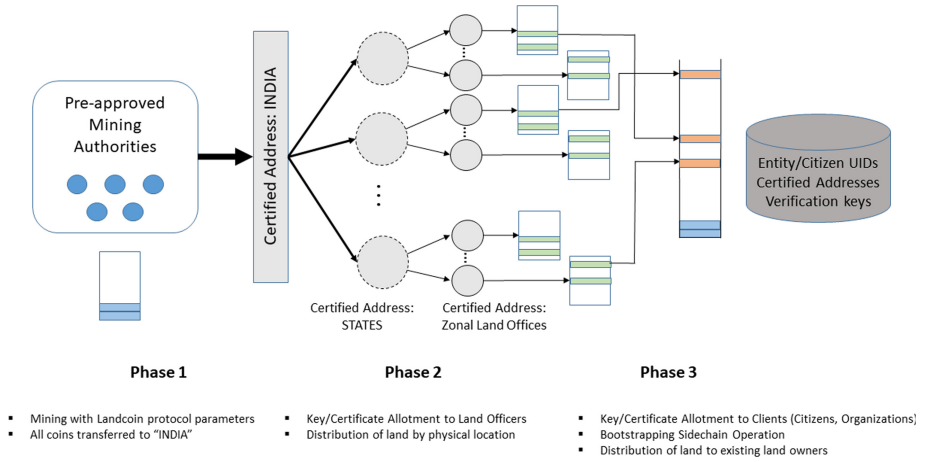

Fig. 1. Landcoin: protocol initialization phases (bootstrapping)

3.2 From Permissionless to Permissioned Setup

Since land ownership is a legal statute backed by the state, the state acts as an arbitrator for all land transactions. To incorporate this requirement, we need to restrict the transaction miners who are authorized to commit transactions to the blockchain. We introduce a role called the "Government Authority" that is allowed to manage the chains by controlling the body of miners. We introduce a special type of transaction called "Governance Transaction" to the mainchain and sidechain where the "Government Authority" can add or remove a public-key from the list of pre-approved miners for their respective chains.

Restricting the nodes who can mine the transactions does away with the concept of incentives for transaction mining. That is, there won't be any transaction fees either on mainchain or sidechain. The coinbase type of transactions that come with the Litecoin protocol are frozen after the completion of Phase 1 in bootstrapping of Landcoin protocol as shown in Fig. 1. Furthermore, the publicly-queriable mainchain only includes transactions that are signed off by the zonal Registrars. This allows for efficient query of land data across the states, while making sure that the control of land data remains with respective states.

In order to build a practical system, the design of the proposed system has to resemble closely the distinct stages in the prevalent land management practices. In the following we enlist the steps involved in a typical land transfer transaction.

3.3 Steps and Requirements of Workflow for Land Management

While there exist several types of land-transfer/mutation transactions: "Sale Deed", "Gift Deed", "Relinquishment Deed", "Partition/Settlement Deed" and "Inheritance/Will Deed"; in this work we explore the "Sale Deed" as a typical

use-case. The protocol can later be extended to accommodate the other deeds and their workflows as well.

The "Sale Deed" is the main document by which a seller transfers his right on the property to the purchaser, who then acquires absolute ownership of the property. The process of "Sale Deed" execution, in Indian context, requires involvement of sellers, buyers, witnesses, land officers, and land registrar at gradual stages. In the following we enumerate the entities, their roles, and the steps in the prevalent land management workflow. These steps are indicative only and they may vary.

1. A *seller* willing to sell property needs to raise an intent to the *Zonal Land Office (ZLO)*.
2. The *ZLO* processes this intent through legal checks and verifies the eligibility of buyer/s.
3. If the intent is allowed to go through, the *ZLO* declares a minimum *Market Value (MV)* for the piece of the land.
4. Upon mutual identity verification, both the parties may negotiate an agreeable price, which is equal to or higher than the *MV*.
5. Then seller prepares a *Transfer of Ownership* document with particulars of the buyer, the land, the price, and two *witnesses* who need to sign it.
6. Revenue tax is calculated for the property and the invoice is presented to the buyer in order to proceed with the land transfer.
7. An invoice is prepared with the details of the parties involved in the transaction, along with a list of conditions that need to be honored.
8. The final invoice, along with two witnesses, is jointly presented to the *Registrar* for approval.
9. As a final step the "Sale Deed" is said to be executed by making the payment of full amount specified in the deed.

Taking into consideration the above indicative workflow for transactions in land management, it is amply evident that several stakeholders carry out intermediate transactions leading to the actual land transaction. Therefore, it is not straightforward to use the *transfer-of-value* type of transaction available under Litecoin protocol. Hence, we need to introduce new transaction types to accommodate representation of intermediate transactions by respective stakeholders.

3.4 Mainchain: Parameters and Construction

We have modified the Litecoin codebase with the following parameters so that we resemble closely with the prevalent land management system and its workflow.

- Total coinbase $\mapsto$ total landmass in India (km^2)
- Divisibility: 8 decimal places (smallest unit is dm^2)
- Block generation time on mainchain: approx. 1 h
- Number of block confirmations: 40 (approx. 1.5 days)
- Consensus: proof-of-work (by pre-approved miners)

We start mining with lower difficulty levels and do not open the blockchain for public participation, until all blocks are mined by the appointed miners. We call this chain as Landcoin's MAINCHAIN. Before initializing it for land transfer, all the miners send their coinbase to the "Government Authority", represented by a self-certified public key. The "Government Authority" then transfers proportionate amounts of Landcoins to individual state Registrars, represented by addresses that are certified by the "Government Authority". The Registrars map the coins to unique URIs of the pieces of land in their respective jurisdictions. The mapping is a transfer operation on the MAINCHAIN to the individual owners of respective URIs. The "Government Authority" invokes "Governance Transaction" (detailed in Sect. 3.6) to authorize a list of public-keys as pre-approved miners. Upon completion of the bootstrapping phase, the MAINCHAIN starts accepting asset-transfer requests.

An asset-transfer transaction, floated by a user on the MAINCHAIN, is accepted by the miners only when it has a signature of the Registrar of the sidechain for the corresponding zone. The attestation process requires the intent transaction to go through pre-defined set of steps as deemed suitable by respective states. Each transaction type on sidechain corresponds to a distinct step in the prevalent workflow for land management.

3.5 SIDECHAIN: Placeholder for Private Information

Though the confirmed transactions on MAINCHAIN show the current ownership of a piece of land and its transactional history, the details about each necessary clearance, attestation, price, et al. are protected from public access. Only the pre-approved public-keys (Registrar, land officers from ZLO) and the parties to the transaction can decrypt the content of the transactions on the sidechain. This provides the property of conditional confidentiality to the content of transactions on the sidechain. We use a CPABE scheme [7] to achieve this property, whose setup and primitive operations are depicted in Fig. 2. The setup for CPABE starts with a global public encryption key (EK) and a master secret key (MSK) that is private to the "Government Authority". For each user of the system, depending upon their roles, certain 'attributes' are defined for which each user has an assigned 'value'. The MSK is used to derive decryption keys for each user according to their 'attribute:value' pairs. For encrypting a message under this scheme, EK is used along with an encoding of the 'Policy Tree', which is a propositional logic statement with 'attribute:value' pairs as their atomic parts (leaves of the tree), always evaluating to either true or false. The encryption algorithm encodes this policy into the resultant ciphertext. During decryption, the ciphertext and the user's key is input to the algorithm and the plaintext is output only if the policy evaluates to true on the user's attribute values. Encryption scheme in [7] is based on bilinear pairings and its implementation is publicly available as a library and documented in [6].

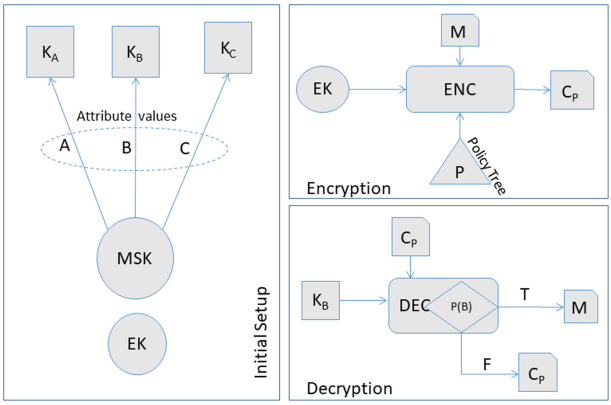

Fig. 2. Ciphertext-policy attribute based encryption [7]

The MAINCHAIN stores all the confirmed *Transfer of Ownership* transactions, and "Governance Transactions"; whereas, the SIDECHAINS (one for each *ZLO*) store the transactions involved in the intermediate steps and run verification scripts for legal compliance. The scripts for compliance check obey the governance policies and are tailored to the workflow for land management of a state.

3.6 Protocol Stakeholders, Their Roles, and Transaction Types

Stakeholders and their roles

Clients (buyers, sellers, witnesses): Buyers and sellers are the end users of the system. Witnesses provide consent to a transaction by digitally signing it.

- Certified Address mapped to Identification info.
- Mainchain Visibility - all information
- Sidechain Visibility - all transactions in which they are a party
- Signing key to use for certain sidechain transactions as seller or witness

Zonal Land Officers: Verification, approval of transaction initiated by sellers, and mining of transactions on SIDECHAIN.

- Mainchain Visibility - all information
- Sidechain Visibility - all sidechain information of her zone
- Signing certain sidechain transactions, and all blocks on the sidechain

Registrar: responsible for final approval of change of ownership requests.

- Certificate Authority defining Land Officer set
- Mainchain Visibility - all information
- Sidechain Visibility - all sidechain information of her region
- Signing key to use for certain sidechain transactions, and mainchain change-of-ownership transactions

Government Authority: maintenance of the system through bootstrapping and "Governance Transactions".

- Certificate Authority defining mainchain miners set
- Trusted Party assigning all clients certified addresses
- Trusted Party assigning all entities CPABE keys
- Mainchain Visibility - all information
- Sidechain Visibility - all transactions in all sidechains
- Signing key to use for governance transactions

Pre-approved Miners: accept and mine the "Change of Ownership" transactions emanating from SIDECHAINs.

- Mainchain Visibility - all information
- Verify all mainchain transactions
- Signing key to use for blocks on the mainchain

Key management and certified addresses

The CPABE master key MSK lies with the "Government Authority" and the encryption key EK is globally known and stored in the Software Interfaces of the Clients, ZLOs, and Registrars. Each of their decryption keys are also derived from this, as shown in Fig. 3. The signing keys and addresses are certified by a TTP that is again, the "Government Authority". These certified addresses are created as in [4] that follows a Diffie-Hellman-like exchange between the client and TTP to generate a shared randomness used to create the Signing Key and certificate. The verification key and address is then derived from it. The certificate is also verified during the signature verification to ensure the key was certified. This computation happens in such a way that the TTP has no knowledge of the final key and so cannot abuse the signing authority of the client.

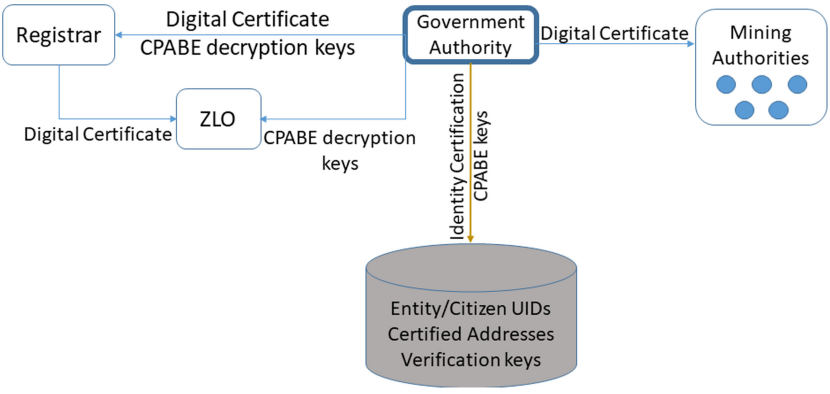

Fig. 3. Key management among the stakeholders

Transaction types and their composition

1. Change of ownership transaction: T_M
   - H_M - Transaction Header
   - $H_{M'}$ - Header of Source transaction on MAINCHAIN
   - $\{A_S\}$ - Certified Addresses of all sellers
   - $\{A_B\}$ - Certified Addresses of all buyers
   - $\{URI\}$ - Survey numbers and GIS co-ordinates
   - DT - Effective-on date
   - S_R - Signature of the Registrar
2. Governance transaction: T_G
   - H_G - Transaction Header
   - $\{A, O, O_i\{\dots\}\}$ -
     - A - Action (add/delete)
     - O - Object (certificate, miner, zone, ttype)
     - $O_i\{\dots\}$ - set of objects
   - EJ - Effective-on jurisdiction
   - DT - Effective-on date
   - S_G - Signature of Government Authority
3. Booking transaction: T_B - Declaration by seller expressing desire to sell land to particular prospective buyer
   - H_B - Transaction Header
   - $H_{M'}$ - Header of Source transaction on MAINCHAIN
   - $\{A_S\}$ - Certified Addresses of all sellers
   - $\{A_B\}$ - Certified Addresses of all buyers
   - $\{URI\}$ - Survey numbers and GIS co-ordinates
   - $\{S_S\}$ - Signatures of sellers
4. Rejection: T_R - Abort of process "Change of Ownership"
   - H_R - Transaction Header
   - $H_{M'}$ - Header of Source transaction on MAINCHAIN
   - RR - Reason for rejection (optional)
   - S_R - Signature of the Registrar
5. Clearance: T_C - Permission to sell at/above declared MV
   - H_C - Transaction Header
   - $H_{B'}$ - Transaction Header of T_B
   - MV - Minimum market value evaluated by ZLO
   - S_L - Signature of ZLO
6. Pre-handover document: T_D - Document declaring final selling price decided upon and identities of witnesses signing off on the handover

- H_D - Transaction Header
- $H_{C'}$ - Transaction Header of T_C
- $\{A_S\}$ - Certified Addresses of all sellers
- $\{A_B\}$ - Certified Addresses of all buyers
- $\{A_W\}$ - Certified Addresses of all witnesses
- $\{URI\}$ - Survey numbers and GIS co-ordinates
- SP - Final selling price
- $\{S_S\}$ - Signatures of sellers

7. Rejection of Pre-handover document: T_{DR}
   - H_{DR} - Transaction Header
   - $H_{D'}$ - Header of Source T_D
   - RR - Reason for rejection (optional)
   - S_L - Signature of ZLO
8. Document verification: T_V - Acknowledgement after verification of legal documents by ZLO
   - H_V - Transaction Header
   - $H_{D'}$ - Header of T_D
   - $\{D_S\}$ - Hashes for doc. clearance of all sellers
   - $\{D_B\}$ - Hashes for doc. clearance of all buyers
   - $\{D_W\}$ - Hashes for doc. clearance of all witnesses
   - S_L - Signature of ZLO
9. Tax Receipt: T_T
   - H_T - Transaction Header
   - $H_{V'}$ - Header of T_V
   - $\{URI\}$ - Survey numbers and GIS co-ordinates
   - SP - Final selling price
   - Tax - Tax amount payable
   - $\{D_T\}$ - Hashes for doc. proof of tax payment
   - S_R - Signature of the Registrar
10. Completion Receipt: T_F
    - H_F - Transaction Header
    - $H_{T'}$ - Transaction Header of T_T
    - $\{A_S\}$ - Certified Addresses of all sellers
    - $\{A_B\}$ - Certified Addresses of all buyers
    - $\{A_W\}$ - Certified Addresses of all witnesses
    - $\{URI\}$ - Survey numbers and GIS co-ordinates
    - SP - Final selling price
    - $\{S_S\}$ - Signatures of sellers
    - $\{S_W\}$ - Signatures of witnesses
    - S_R - Signature of the Registrar

Mainchain blocks include transactions of type T_M and T_G. All the other types of transactions appear on the sidechain. The 8-step land transfer transaction is depicted in Fig. 4.

noend 1. Landcoin Protocol

1: Seller initiates T_B on SIDECHAIN
2: ▷ refers to previous T_M that acts as an anchor
3: **if** Legal conditions of exchange are not met **then**
4: Registrar puts T_R **return**
5: **else**
6: *ZLO* puts T_C with mention of *MV*
7: Seller puts T_D with final price and Witnesses
8: **while** *ZLO* puts T_{DR} **do**
9: **if** Still interested **then**
10: Seller re-does T_D
11: **else**
12: T_R **return**
13: **while** Document Verification not approved by *ZLO* **do**
14: **if** Still interested **then**
15: **if** Valid documents can be produced **then**
16: *ZLO* puts T_V
17: **else**
18: Seller re-does T_D
19: GOTO line 9
20: **else**
21: T_R **return**
22: T_T is put on the SIDECHAIN
23: T_F is put on the SIDECHAIN
24: T_M is put on the MAINCHAIN **return**

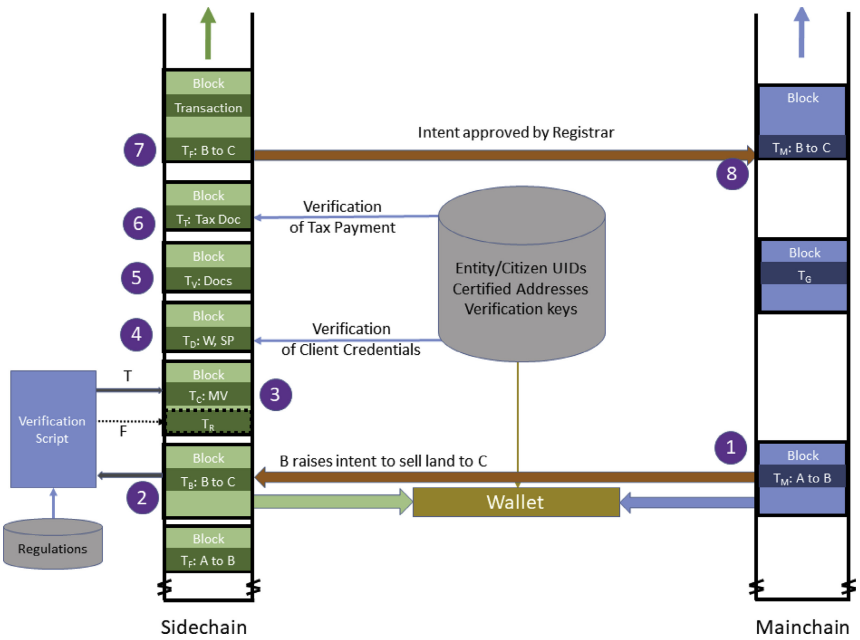

Fig. 4. Land transfer transaction in Landcoin system

4 Summary of Guarantees

This system aims to provide the following guarantees:

Authenticated Yet Pseudonymous Clients. Certified Addresses provided by the Government Authority are conditioned on verification of the identity of the client as an actual and unique real-world entity. This is a one-time process and helps in keeping track of the userbase of the system with legal implications. The addresses do not reflect user IDs on chain and so the protocol henceforth is a pseudonymous; one with only the certificates being verified on chain.

Verify-Able History of Land Transactions. All the MAINCHAIN transactions originate from the Government Authority address and thus all the existing land is accounted for. Furthermore, all valid change-of-ownership transactions are signed by the Registrar (having gone through the entire SIDECHAIN workflow) before committing on the MAINCHAIN. This consolidated transaction-trail provided by the Landcoin system, along with the queryable MAINCHAIN transactions, mitigates double-spend/ownership frauds.

Confidentiality of Intermediate Steps. All intermediate steps for the change of ownership transaction are recorded on the SIDECHAIN. This maintains a consolidated record of all the actions/approvals taking place and, at the same time, keeps unnecessary details outside of the MAINCHAIN. As these transactions use private information like identity, payment, tax-status for verification; they are encrypted under CPABE for authorized access.

Honesty Among Mining Authorities. All mining authorities are regulated: added and evicted, if needed, by the Government Authority; thus categorizing our system as a permissioned blockchain. While competition still exists among them for any off-chain compensation the Government Authority may provide, malicious miners risk being identified and their authority being revoked. Therefore, minimal, if any (only theoretically), forking can be expected; but in the event of one, it may eventually get resolved due to the slow growth of the chain. Nevertheless, as any transaction put on the chain needs to come signed by the Registrar, a fork will not translate to a double-spend event!

Centralized Authority with Decentralized Auditability. The proposed protocol does not deviate the prevalent structure of centralized authority at the state-level for land record management. However, it facilitates inclusion of users at national-level through public auditability and verification by querying the public MAINCHAIN.

5 Implementation Details

Fig. 5. Landcoin wallet: login window and different user roles

As a proof-of-concept we modified [2] the Litecoin codebase and designed QT-based wallet to interact with the Landcoin blockchain system. This implementation supports four roles: Client (Individual or Organization), Registrar (with operations of ZLO), Government Authority, and Miners. Figure 5 shows the Login/Registration screen.

Each Landcoin Client has a unique client ID that needs to be entered into the Login Window along with a password. When a new Client registers, his/her certified keys and address is then generated by a back-end call to the Trusted Third Party.

A Client can use View Menu to explore the MAINCHAIN, to see the list of ongoing transactions he/she is involved in, and the list of his/her completed transactions. Upon approval, the transaction then becomes part of the USER-MEMPOOL. The Registrar's Dashboard contains his credentials that are similar to that of the Client's except it also includes the Zone of jurisdiction Fig. 6. This role has permissions to view all the MAINCHAIN transactions using the chain explorer(wallet), ongoing transactions of the zone, completed transactions of the zone, and current zone state (current owners of land in the zone). This includes transactions in the USERMEMPOOL, the MEMPOOL, and and the UTXO that belong to the zone. As in the prevalent practice, the Registrar performs the role of giving the final approval for any transaction. This transaction then is moved from the USERMEMPOOL to the MEMPOOL from where it can be picked up by a miner to be included in a block on the blockchain.

A Miner, once logged in, can view the MEMPOOL, UTXO and the blockchain through the explorer. However, mining is not possible unless a special permission is granted by the Government Authority. The Government Authority can always traverse through the MAINCHAIN and SIDECHAINs. It also has a view (shown in Fig. 8) of the list of approved miners and prospective miners that have requested mining permission. The TTP for the certified address generation is implemented

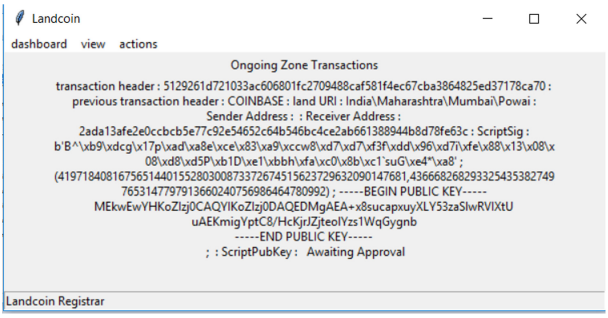

Fig. 6. Registrar view: ongoing transaction of the zone

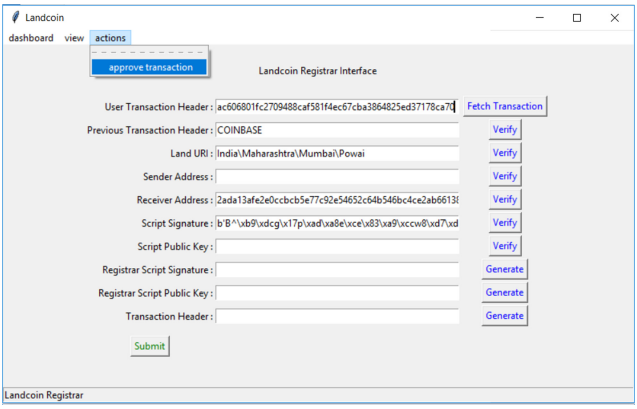

Fig. 7. Registrar action: approve transaction

as a python function that interacts with the clients as a separate entity during user registration. It performs automated checks with an existing database and does not explicitly need human intervention. It can be optionally merged with the Government Authority though an interface for the same is not provided. Furthermore, the op-code set is extended (as in the certified addresses specification) to include an op-code for verification for white-listed certificates/keys (permissioned entities). We are also exploring integration of Geohash [1] and Cadastral maps [3] in our implementation to provide a realistic view of land management to the stakeholders (Fig. 7).

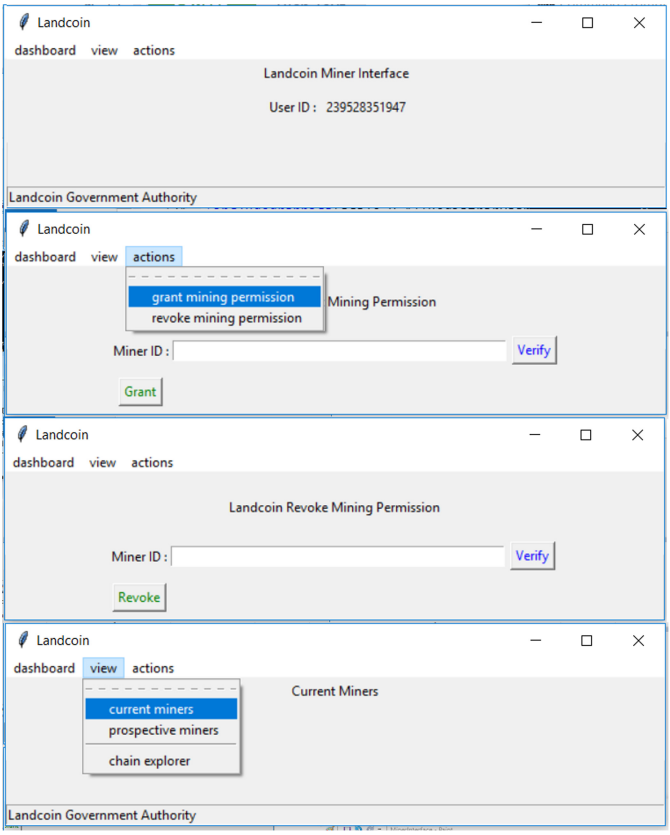

Fig. 8. Government authority interface

6 Conclusion

We have devised Landcoin – a practical *transfer-of-asset* system based on a proven & tested system for *transfer-of-value*. Landcoin extends the limited and secure opcode set of Litecoin codebase. This set is Turing incomplete and all the scripts written can be formally verified for correctness, at the same time providing just enough functionality for our use-case. Transaction details are segregated into public and private data streams on separate but intertwined blockchains, helping us preserve privacy of individual transaction details. The Mainchain records each and every successful transfer of ownership transaction, and the Sidechain records the intermediate details of such transactions emanating from the Mainchain. Thus, anyone can browse through the Mainchain ledger to verify the ownership of land but the intricate details of associated ownership provenance are available only to the stakeholders of that transaction. Confidentiality of transaction details on the Sidechains are enforced using CPABE (Ciphertext Policy - Attribute Based Encryption) scheme, where the "Government Author-

ity" possesses the master key so it can read any transaction, which is also the case in current process of land management in India. Our system closely imitates the process prevalent for land management in Indian states while improving transparency in the system and providing privacy at the same time! Privacy and transparency are orthogonal properties. We would be analysing pros and cons of upcoming digital asset management systems like NFT (Non-Fungible Tokens) [10].

Acknowledgements. We would like to thank Anasuya Acharya and Bajrang Sutar who worked on this project.

References

1. Geohash. http://geohash.org/site/tips.html
2. How to create a new altcoin. https://bitcointalk.org/index.php?topic=225690.0
3. Standard on Manual Cadastral Maps and Parcel Identifiers. https://www.iaao.org/media/standards/Manual_Cadastral_Maps_2016.pdf
4. Ateniese, G., Faonio, A., Magri, B., de Medeiros, B.: Certified bitcoins. In: Proceedings of Applied Cryptography and Network Security - ACNS, pp. 80–96 (2014)
5. Atzei, N., Bartoletti, M., Cimoli, T.: A survey of attacks on Ethereum smart contracts (SoK). In: Maffei, M., Ryan, M. (eds.) POST 2017. LNCS, vol. 10204, pp. 164–186. Springer, Heidelberg (2017). https://doi.org/10.1007/978-3-662-54455-6_8
6. Bethencourt, J., Sahai, A., Waters, B.: Advanced crypto software collection - cpabe (2006)
7. Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-policy attribute-based encryption. In: 2007 IEEE Symposium on Security and Privacy (S&P 2007), pp. 321–334 (2007)
8. Cachin, C.: Architecture of the Hyperledger Blockchain Fabric (2016). https://www.zurich.ibm.com/dccl/papers/cachin_dccl.pdf
9. eMudhra: Case Study: land records securely on a Blockchain. https://www.emudhra.com/us/case-studies/blockchain/emBlock_land_records_case_study.pdf
10. Ethereum. Non-fungible tokens (NFT) (2021). https://ethereum.org/en/nft/,
11. Karnataka Government. https://landrecords.karnataka.gov.in
12. Abhishek, G.: Property registration and land record management via blockchains. https://security.cse.iitk.ac.in/sites/default/files/2019-09/14807257.pdf
13. Kalra, G., Goel, S., Dhawan, M., Sharma, S.: ZEUS: analyzing safety of smart contracts. In: 25th Annual Network and Distributed System Security Symposium, NDSS (2018)
14. Labs, R.: Run rippled as a validator (2021). https://xrpl.org/run-rippled-as-a-validator.html
15. Litecoin. The cryptocurrency for payments (2011). https://litecoin.org/
16. Mishra, P., Suhag, R.: Land records and titles in India (2017). http://www.prsindia.org/uploads/media/Analytical
17. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system (2008). http://bitcoin.org/bitcoin.pdf
18. Shyamasundar, R.K., Patil, V.: Blockchain: the revolution in trust management. Proc. Indian Natl. Sci. Acad. **84** (2), 385–407 (2018)

19. Thakur, V., Doja, M.N., Dwivedi, Y.K., Ahmad, T., Khadanga, G.: Land records on blockchain for implementation of land titling in India. Int. J. Inf. Manag. **52**, 101940 (2019)
20. Wood, G.: Ethereum: a secure decentralised generalised transaction ledger EIP-150 REVISION (2017)