Landcoin - A Land Management Protocol

Anasuya Acharya
Information Security Research and Development Center
Department of Computer Science and Engineering
Indian Institute of Technology Bombay, Mumbai 400076, India
Email: anasuyahirai@gmail.com

***Abstract*—Public blockchains provide integrity, transparency, immutability, and inclusion-guarantee to the transactions they process and record in their chain of blocks. Bitcoin, Litecoin are a few examples of time-tested, reliable public blockchains that handle only one type of transaction i.e., transfer-of-value (specifically money/currency) from a user to another. Whereas, general purpose blockchains like Ethereum provide means and methods to encapsulate transfer of not only a value but any asset class that can be digitally represented. However, due to its high-level programming language to write asset transfer rules, Ethereum has encountered instances where it had to forgo the claim of immutability (e.g., the DAO attack). On contrary, the purpose-built, script-based blockchains like Litecoin have withstood the test of time and therefore are seen as reliable – an important aspect in attracting users to use a system that is built using such proven, reliable protocols. In this paper, we present an *asset-transfer* 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 integrate *sidechains* to store transaction details that are private to the transacting parties, thus providing conditional privacy to the transactions. The *mainchain* stores land records that can be queried by the public, whereas sidechains are integrated to store the intricate details about the intermediate validations/operations performed by regulators, registrars, and notaries.**

***Index Terms*—blockchain, Litecoin, land management, privacy.**

I. 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 [9]. 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 [1] 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 programs supported by the underlying blockchain), which inherit the pros and cons of any high-level programming language [3]. Another forthcoming limitation of these 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.

II. Background & 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 [11]. 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 of actions. 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 of transactions in the system.

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 [8] 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 could be used but its underlying programming language may open up avenues [3], [7] for serious asset loss or inconsistent asset ownership states, which is unacceptable. Therefore, we believe that it is prudent to extend a protocol (like Bitcoin [10] or Litecoin [8]) that is built for a specific purpose rather than using a general purpose protocol like Ethereum [12] or Hyperledger Fabric [6]. Between the Bitcoin and the Litecoin codebases, 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 blockchain protocol. In summary, the following are the modifications we introduced in the Litecoin protocol, for which we present details in the next Section.

1) New transaction types: for mainchain and sidechain, each corresponding to a step in the current workflow of land management
2) Pre-approved miners: 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) Certified coins and mapping of coins to the 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 user 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 cryptocurrencies, a Trusted Third Party (TTP) is involved in verifying identities and assigning certificates with the keys being formed jointly by both parties.
   The protocol in [2] is still pseudonymous and the TTP has no control over the transactions being signed, but this helps keep track of the mapping of users in the systems against their existence as real-world entities.

III. Architecture of Landcoin Protocol

This section is a guide through all the design aspects taken into consideration while creating the Landcoin Protocol.

A. 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.

B. 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

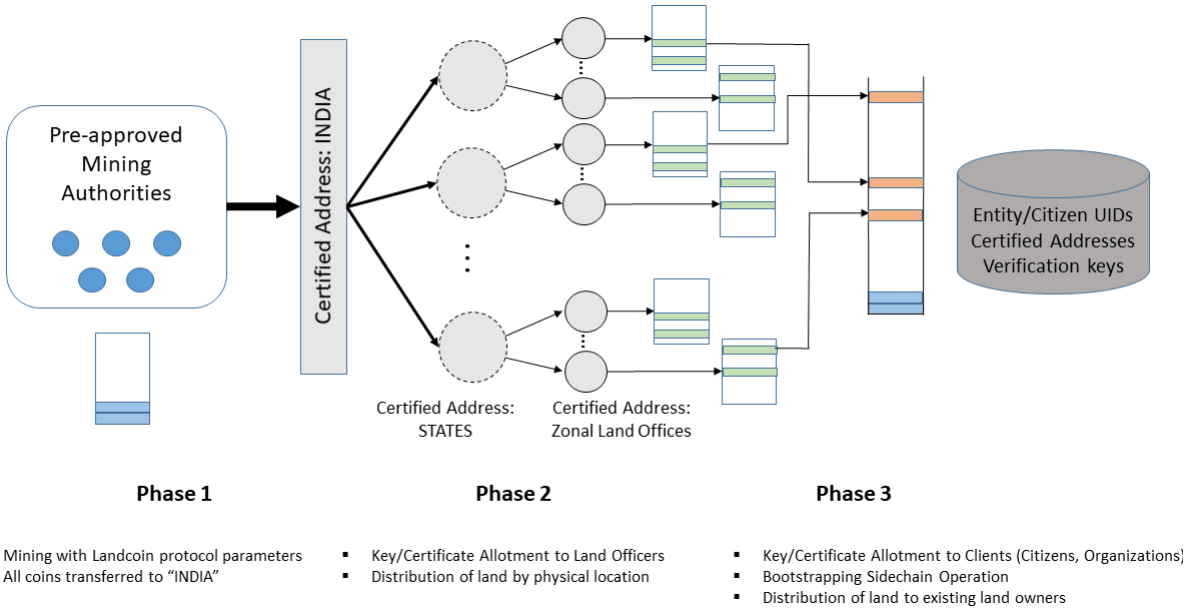

Fig. 1. Landcoin Protocol Initialization Phases (Bootstrapping)

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 Figure 1.

Furthermore, the publicly-queriable mainchain only includes transactions that are signed off by the zonal Registrars. This makes allows for efficient queries from data across states, while making sure that the power remains with the state. Furthermore, this serves as an abstraction for any intermediate steps involved that are encapsulated as confidential transactions on the sidechains.

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.

C. Steps & requirements of the land transaction workflow

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 work-flows 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 the document.
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 of intended land transfer leading to a valid "Sale Deed" execution.
9) As a final step the "Sale Deed" is said to be executed by making the payment of full amount specified in the deed.

This payment amount constitutes the revenue tax.

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.

D. 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 hour
- 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 Section **??**) 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 process.

E. 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 hidden from the public. 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 [5] to achieve this property, whose setup and primitive operations are depicted in Figure 2.

The setup for CPABE starts with a globally public encryption key (EK) and a master secret key (MSK) that is private

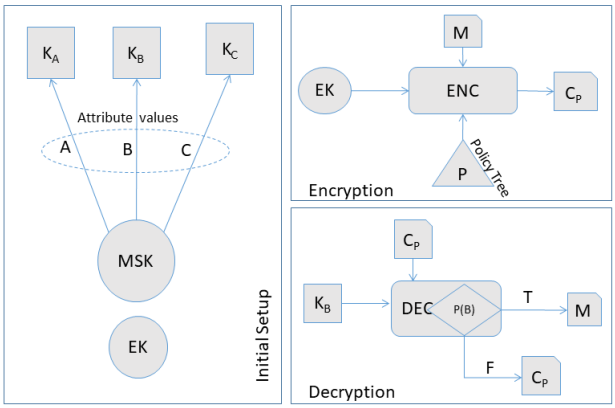

Fig. 2. Ciphertext Policy - Attribute Based Encryption [5]

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 [5] is based on bilinear pairings and its implementation is publically available as a library and documented in [4].

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 special purpose – specific to the land resource management of a state.

F. Protocol Stakeholders, their Roles, and Transaction Types

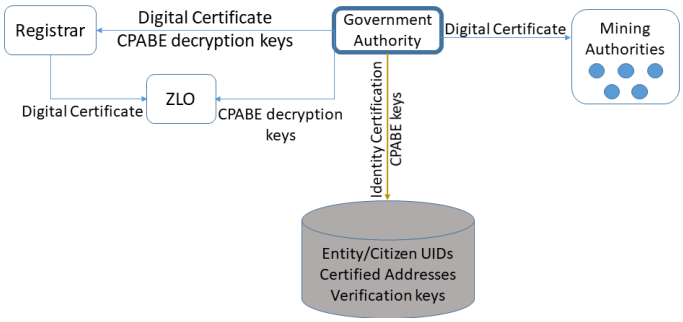

Fig. 3. Key management among Stakeholders

Stakeholders and their roles:

- *Clients (buyers, sellers, witnesses):* Buyers and sellers are the end users of the system. Witnesses provide consent to a specific transaction by digitally signing it.
  - Certified Address mapped to Identification info.
  - Mainchain Visibility - all information
  - Sidechain Visibility - all transactions in which they are a buyer, seller, or witness
  - 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 info. of that office
  - Signing key to use for certain sidechain transactions, and all blocks for 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 info. of that office
  - 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 Figure 3.

The signing keys and addresses are certified by a TTP that is again, the "Government Authority". These certified addresses are created as in [2] 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.

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*

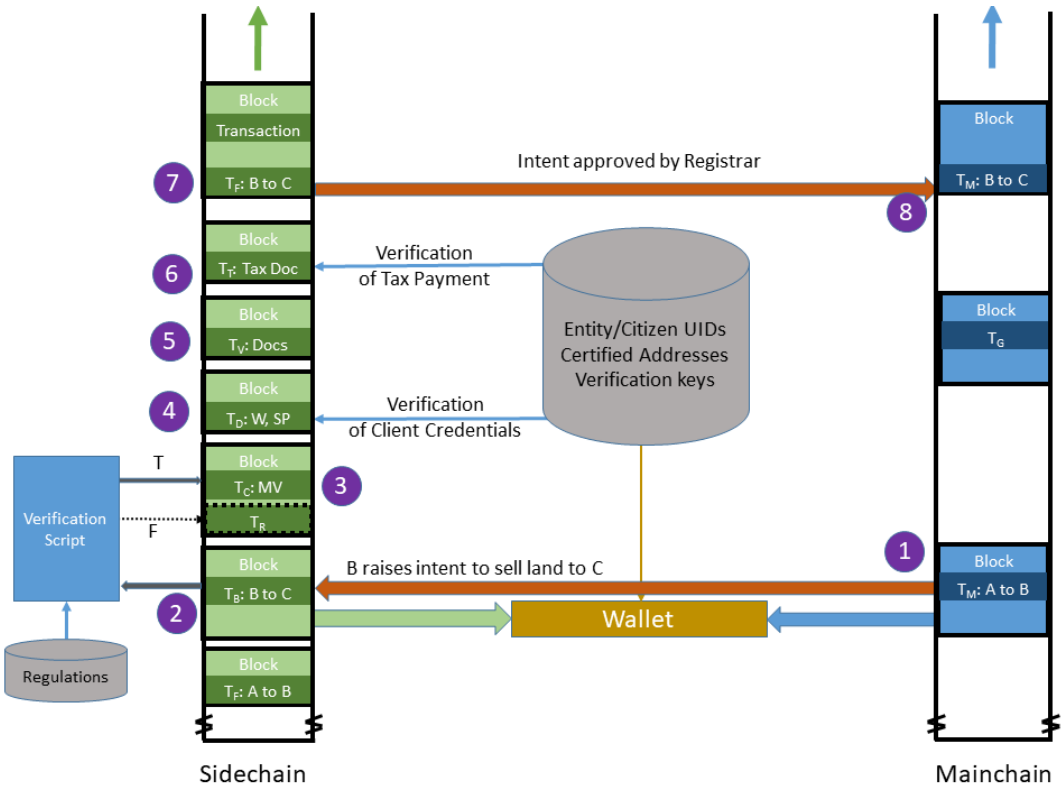

Fig. 4. Land Transfer Transaction in Landcoin

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

IV. Summary of Guarantees

This system aims to provide the following guarantees:

1) Authenticated yet Pseudonymous Clients: Certified Addresses provided by the Government Authority is 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 keep track of the user base of a system with legal implications such as this one. 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.

2) Verify-able history of Land Transactions: MAINCHAIN transactions all originate from Government Authority address and so 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 being put on the MAINCHAIN. This consolidated transaction trail provided by the blockchain, along with the queryable booking transactions, mitigates double spend frauds.

3) Confidentiality of Intermediate Steps: All intermediate step transactions for change of ownership are recorded on the SIDECHAIN. This maintains a consolidated record of all the actions taking place and, at the same time, keeps unnecessary details outside of the MAINCHAIN. As these transactions use confidential information like identities for verification and such, they are encrypted under CPABE for proper access control to be maintained.

4) Honesty among Mining Authorities: All mining authorities are regulated: added and evicted, if needed, by the

Algorithm 1 Landcoin Protocol

Seller initiates T_B on SIDECHAIN
    ▷ refers to previous T_M that acts as an anchor
if Legal conditions of exchange are not met **then**
    Registrar puts T_R **return**
else
    ZLO puts T_C with mention of *MV*
    Seller puts T_D with final price and Witnesses
    while *ZLO* puts T_{DR} **do**
        if Still interested **then**
            Seller re-does T_D
        else
            T_R **return**
        end if
    end while
    while Document Verification not approved by *ZLO* **do**
        if Still interested **then**
            if Valid documents can be produced **then**
                ZLO puts T_V
            else
                Seller re-does T_D
                GOTO line 9
            end if
        else
            T_R **return**
        end if
    end while
    T_T is put on the SIDECHAIN
    T_F is put on the SIDECHAIN
    T_M is put on the MAINCHAIN **return**
end if

Government Authority and therefore one can expect minimal malicious activity. While competition still exists among them for any off-chain compensation the Government Authority may provide malicious miners can have their authority revoked. Therefore, minimal, if any, forking can be expected; but in the event of one, it may take as much as over a day to resolve 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.

5) Centralized Authority with Decentralized Auditability: The protocol allows for as less deviation form the existing structure of authority for land record management as possible. However, it facilitates larger inclusion of both users and land charted; and ease of auditability and verification by virtue of the guarantees provided by the blockchain structure and its underlying cryptographic basis.

V. Implementation Details

As a simplified proof-of-concept, the following is an implementation of the protocol. This implementation supports four roles: Client (Individual or Organization), Registrar (with operations of ZLO), Government Authority, and Miners.

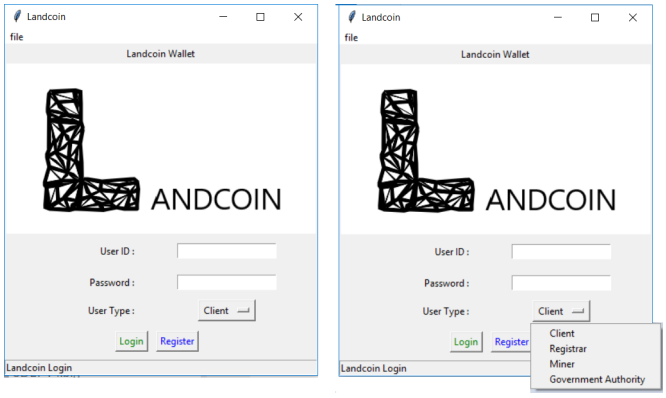

Fig. 5. Login Window and Different User Roles

A Landcoin Client has a client ID that needs to be entered into the Login Window along with a password. If a new Client registers, his/her certified keys and address is then formed by a back-end call to the Trusted Third Party. Given below are the typical client credentials:

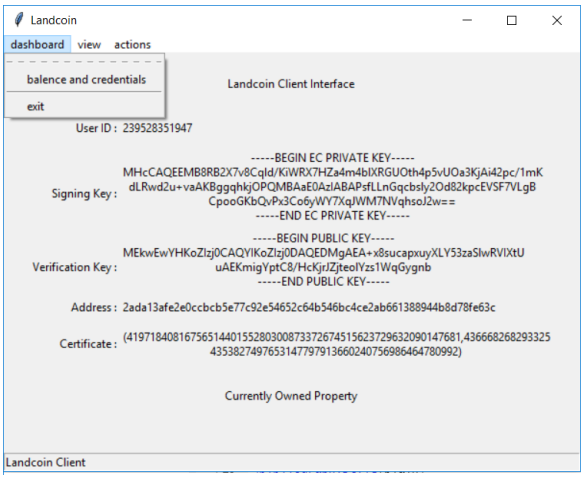

Fig. 6. Client Dashboard

A client can view, using the View Menu, the chain explorer of the mainchain, list of ongoing transactions he/she is involved in, list of his/her completed transactions within the system.

Fig. 7. Client View: Ongoing Transactions of the Client

Furthermore, in this simplified version, creation/initiation of the transaction and all the steps after it is merged into one action that the client performs. This transaction then becomes part of the USERMEMPOOL.

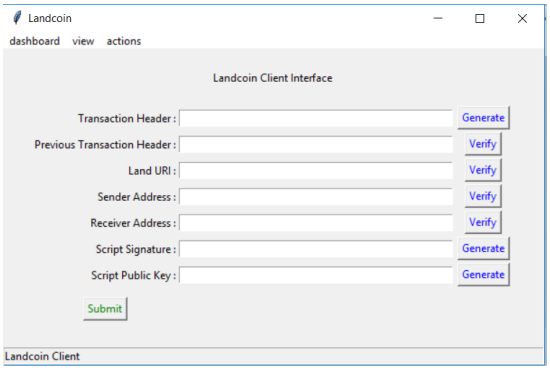

Fig. 8. Client Action: Initiate New Transaction

The Registrar's Dashboard contains his credentials that are similar to that of the Client's except it also includes the Zone of jurisdiction.

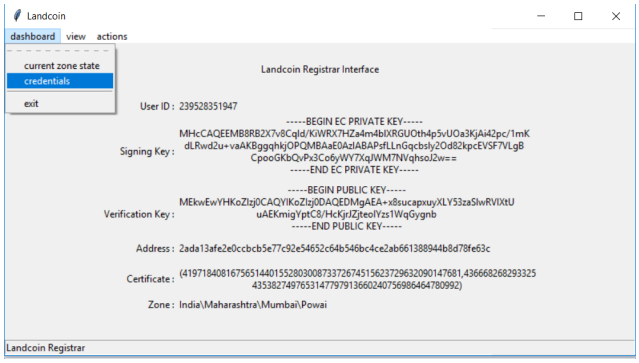

Fig. 9. Registrar Dashboard

This role has permissions to view all mainchain transactions through the chain explorer, 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.

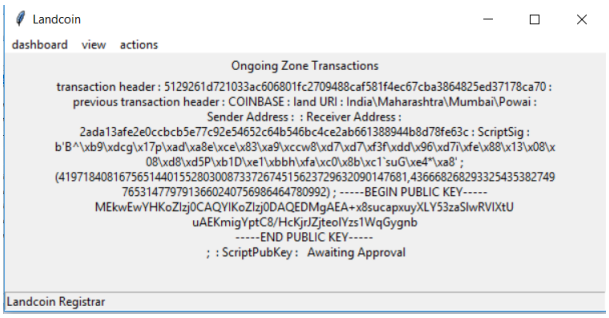

Fig. 10. Registrar View: Ongoing Transaction of the Zone

As in the original protocol, the registrar also reserves 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.

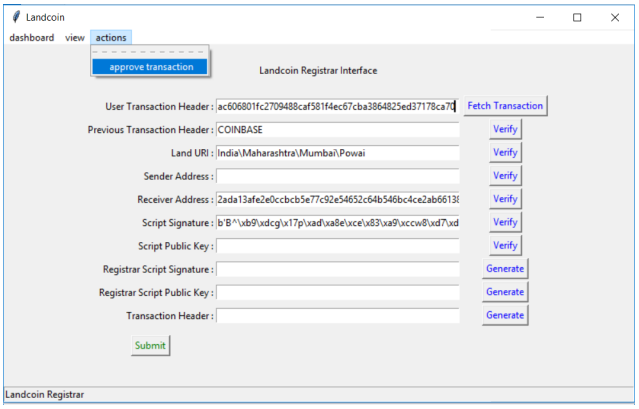

Fig. 11. Registrar Action: Approve Transaction

The remaining two interfaces are of the Miner and the Government Authority. 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 actions that a Miner can perform are requesting for mining permission, and mining (once the permission is granted).

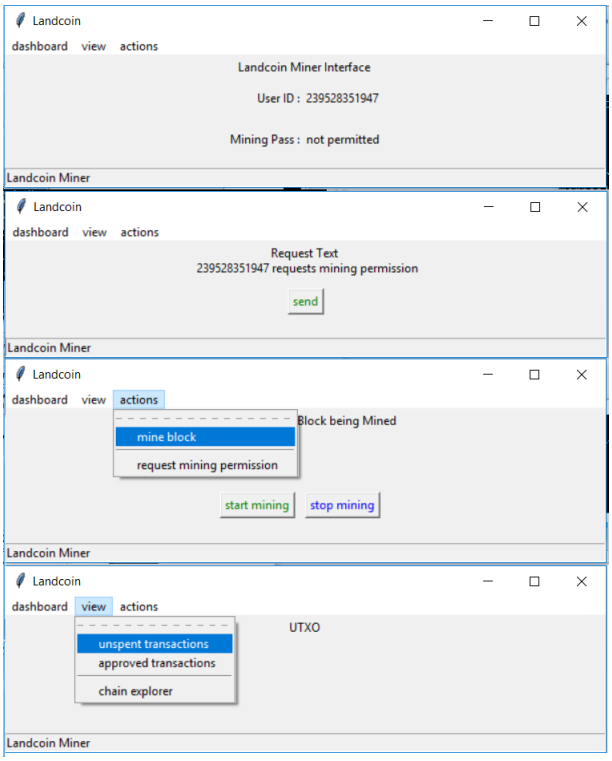

Fig. 12. Miner Interface

The Government Authority is allowed access to the main blockchain through the explorer, and can view the list of current miners and prospective miners that have requested permission for the same. The actions this role performs include granting and revoking of mining permission.

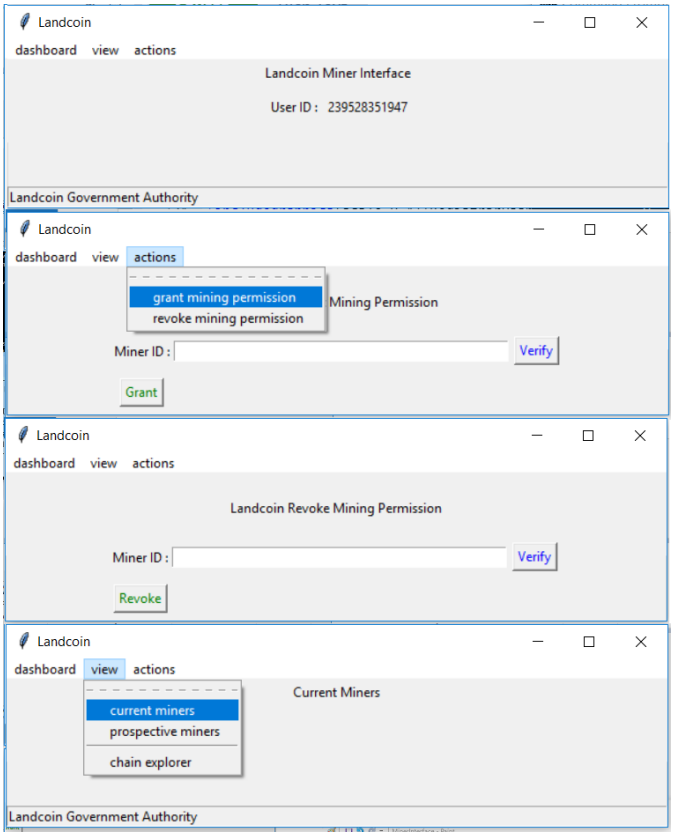

Fig. 13. Government Authority Interface

The TTP for the certified address generation is implemented 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 by one (as in the certified addresses specification) to include an op-code for verification for certificates.

VI. Conclusion

We have devised a *transfer-of-asset* system (Landcoin) from a *transfer-of-value* system (i.e., Litecoin). Landcoin extends the limited and secure opcode set of Litecoin. 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 linked blockchains, helping us preserve the privacy. Mainchain records each and every successful transfer of ownership transaction, and the sidechain records the intermediate details of such transactions emanating from mainchain. Thus anyone can browse through the mainchain to verify the ownership of land but the intricate details of associated ownership provenance is available only to the stakeholders of that transaction. Confidentiality of transaction details on sidechains is enforced using CPABE (Ciphertext Policy - Attribute Based Encryption) scheme, where the "Government Authority" possesses the master key so it can read (decrypt) any transaction. This is a preliminary version of Landcoin and we are experimenting with different methods to achieve transaction confidentiality and privacy on sidechains.

Acknowledgment:

This work is carried out as part of research at ISRDC (Information Security Research and Development Center), supported through grant 15 DEITY00 004, funded by MeitY, Government of India.

References

[1] https://landrecords.karnataka.gov.in.
[2] Giuseppe Ateniese, Antonio Faonio, Bernardo Magri, and Breno de Medeiros. Certified bitcoins. In *Proceedings of Applied Cryptography and Network Security - ACNS 2014.*, pages 80–96, 2014.
[3] Nicola Atzei, Massimo Bartoletti, and Tiziana Cimoli. A Survey of Attacks on Ethereum Smart Contracts SoK. In *Proc. of the 6th Int. Conf. on Principles of Security and Trust - LNCS 10204*, pages 164–186, 2017.
[4] John Bethencourt, Amit Sahai, and Brent Waters. Advanced crypto software collection - cpabe, 2006.
[5] John Bethencourt, Amit Sahai, and Brent Waters. Ciphertext-policy attribute-based encryption. In *2007 IEEE Symposium on Security and Privacy (S&P 2007)*, pages 321–334, 2007.
[6] Christian Cachin. Architecture of the Hyperledger Blockchain Fabric. https://www.zurich.ibm.com/dccl/papers/cachin_dccl.pdf, 2016.
[7] Sukrit Kalra, Seep Goel, Mohan Dhawan, and Subodh Sharma. ZEUS: analyzing safety of smart contracts. In *25th Annual Network and Distributed System Security Symposium, NDSS*, 2018.
[8] Litecoin. The cryptocurrency for payments. https://litecoin.org/, 2011.
[9] Prachee Mishra and Roopal Suhag. Land records and titles in India. http://www.prsindia.org/uploads/media/Analytical%20Report/Land%20Records%20and%20Titles%20in%20India.pdf, 2017.
[10] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. http://bitcoin.org/bitcoin.pdf, 2008.
[11] RK Shyamasundar and Vishwas Patil. Blockchain: The revolution in trust management. In *Proc. of Indian National Sci. Academy, Vol 84 (2)*, 2018.
[12] Gavin Wood. Ethereum: A secure decentralised generalised transaction ledger EIP-150 REVISION, 2017.