NOVA SCHOOL OF SCIENCE & TECHNOLOGY

DEPARTMENT OF COMPUTER SCIENCE

RODRIGO MIGUEL NEVES AREDE

BSc in Computer Science and Engineering

BLOCKOPOLY

A BLOCKCHAIN-BASED APPROACH TO LAND REGISTRY

Dissertation Plan
MASTER IN COMPUTER SCIENCE AND ENGINEERING

NOVA University Lisbon
February, 2024

DEPARTMENT OF
COMPUTER SCIENCE

BLOCKOPOLY

A BLOCKCHAIN-BASED APPROACH TO LAND REGISTRY

RODRIGO MIGUEL NEVES AREDE

BSc in Computer Science and Engineering

Advisers: Artur Miguel Dias
Assistant Professor, NOVA University Lisbon
André Simões
Product Line Manager, Crossjoin Solutions
Nuno Valente
Architect, Crossjoin Solutions

Co-adviser: Sebastião Mayor
Software Engineer, Crossjoin Solutions

Dissertation Plan
MASTER IN COMPUTER SCIENCE AND ENGINEERING

NOVA University Lisbon
February, 2024

Abstract

Real Estate is a cornerstone of the global economy, representing a significant portion of wealth and being a major factor in any country's GDP. Yet, despite being one of the most important sectors, it is still one of the most outdated. The traditional process of land conveyance is cumbersome, slow, and expensive, primarily due to the fragmentation of information across various controlling entities. There's a need to have this data unified in a single shared database that all the relevant parties may access and contribute, but none fully controls. This study explores the potential benefits of using blockchain technology for this purpose and proposes a novel smart contract architecture for a permissioned blockchain network implemented with Hyperledger Fabric. The presented solution comprises land conveyance and renting functionalities and demonstrates how its application could bring increased efficiency, transparency, and trustworthiness over legacy systems.

Keywords: Real Estate, Land Registry, Blockchain, Smart Contracts

Resumo

O setor imobiliário é um pilar da economia global, representando uma porção significativa da riqueza e sendo um fator crítico para o PIB de qualquer país. No entanto, apesar de ser um dos setores mais importantes, é também um dos mais desatualizados. O processo tradicional de compra e venda de imóveis é complicado, lento e de alto custo, principalmente devido à fragmentação de informação entre as várias entidades que controlam o processo. Há uma necessidade de unificar toda a informação numa base de dados única e partilhada que todas as partes relevantes possam aceder e contribuir, mas que nenhuma controle totalmente. Este estudo explora os potenciais benefícios do uso da tecnologia blockchain para esta finalidade, e propõe uma arquitetura de smart contracts para uma rede "permissioned", implementada com Hyperledger Fabric. A solução apresentada compreende funcionalidades de transferência e aluguer de propriedades, e é demonstrado como a sua aplicação poderia trazer maior eficiência, transparência e confiabilidade em relação aos sistemas tradicionais.

Palavras-chave: Imobiliária, Registo Predial, Blockchain, Smart Contracts

Contents

List of Figures

List of Tables

Acronyms

BFT Byzantine Fault Tolerance *(p. 7)*
BTC Bitcoin *(pp. 6, 9)*

CA Certificate Authority *(pp. 8, 14)*
CFT Crash Fault Tolerance *(p. 7)*

DAO Decentralized Autonomous Organization *(p. 24)*
dApps Decentralized Applications *(p. 9)*

ETH Ether *(pp. 6, 9)*
EVM Ethereum Virtual Machine *(p. 11)*

FCT NOVA School of Science and Technology *(p. 2)*

GDP Gross Domestic Product *(pp. 1, 21)*

IPFS InterPlanetary File System *(pp. 2, 10, 30)*

LLC Limited Liability Company *(pp. 18, 23)*

MSP Membership Service Provider *(pp. 14, 19, 33)*

NFTs Non-fungible Tokens *(pp. 9, 16)*

OCL Object Constraint Language *(pp. 28, 38)*

P2P Peer-to-Peer *(p. 5)*
PKI Public Key Infrastructure *(pp. 8, 14, 27, 30, 33)*
PoCs Proofs-of-Concept *(p. 20)*

PoS Proof-of-Stake *(p. 6)*
PoW Proof-of-Work *(p. 6)*

SPV Special Purpose Vehicle *(pp. 18, 23)*

UML Unified Modeling Language *(pp. 20, 28)*

1

Introduction

Real estate makes up a sizable portion of the world's economic assets - Statista's reports reveal that the value of the worldwide real estate market reached US$613.60tn in 2023 [47]. The land registry system is one of the crucial aspects of any government. Proper land record management is essential for economic growth and governance, as it constitutes a major factor in increasing a country's GDP. Even so, many countries rely on archaic, century-old procedures for managing their land records. In the current days, these outdated methods are increasingly seen as nonsensical and are a source of widespread dissatisfaction. The most commonly spotted flaws are typically related to [44, 45]:

Time - The transfer process may take weeks or even months to complete, due to the complexity of the required procedures;

Cost - Countless expenses and taxes are placed upon the transacting parties due to the involvement of numerous entities, significantly raising the cost of the process;

Complexity - The transacting parties are typically thrown at a labyrinth of never-ending procedures and bureaucracies, often requiring them to physically meet with the involved entities.

Fraud - Having different entities controlling different steps of the process results in a serious lack of transparency and creates opportunities for malicious individuals to exploit the system [24].

Intuitively, the root cause of these flaws lies in the decentralized and fragmented nature of the land conveyance process. Land records are administered by a multitude of entities, including government agencies, legal bodies, real estate agents, and financial institutions [21], each carrying their own roles and purposes. Data and documents necessary for the process completion are scattered across servers of more than one party, often duplicated and stored in different formats [52]. The ideal scenario to solve this problem would be to unify all the data in a single common database [15], following a well-defined standardized structure. The various involved entities should be able to access and modify the database, based on their role and permissions. Furthermore, it is vital that none of the entities fully control the database, since trust between these entities is not a guarantee. Blockchain technology may present a viable solution for this purpose. Blockchain is a decentralized, distributed ledger technology that offers transparency, security, and immutability. For this particular purpose, a consortium-typed permissioned blockchain network would be ideal, as it would enable the referred parties to access a shared database without the need for a central authority while maintaining a level of privacy and confidentiality suitable for sensitive data such as land records.

1.1 Objectives

The primary goal of this work is to study the feasibility of using blockchain technology as the primary infrastructure to store land records. Along the way we will examine the current land record systems, pointing out their main limitations; provide an overview of previous studies and existing implementations, identifying the best practices and standards; and finally, based on the knowledge and insights gained, will propose a novel architecture for a consortium blockchain network using Hyperledger Fabric. The proposed system will primarily focus on supporting functionalities for land conveyance and renting.

1.2 Contributions

The expected contributions from this work are:

1. A report of the existing solutions for real estate property management;
2. The design, implementation, and evaluation of a smart contract architecture for a consortium blockchain network.
3. Network configurations relative to the roles and permissions of the peers participating in it;
4. Configurations for deploying an IPFS network that complements the main blockchain network, with the goal of storing off-chain data;
5. Depending on the time frame, a demonstrative client application may be developed to help showcase the system's capabilities.

1.3 Research Context

The Blockopoly Master Thesis proposal emerges from the collaboration between the academic expertise of NOVA School of Science and Technology (FCT) and the innovation initiatives of Crossjoin, a portuguese-based company created by a small group of experienced engineers mainly focused on the performance optimisation of large enterprise systems. For the last 14 years and since the company's inception, Crossjoin has accumulated consulting expertise and knowledge in various industries, from Telecoms to Finance services and even going through Agriculture verticals. During its life, it increased the surface area of its activities, which now encompass specialised architecture consultancy and software engineering, application and infrastructure support, and overall performance optimisation programs. With a keen interest in the technology that will become mainstream in the following years, Crossjoin started cross-cutting initiatives for their clients with internal product development and technology exploration. These initiatives allow the company to experience the hardship of newly introduced technologies and work toward optimal insertion and maintenance paths. Crossjoin believes that its innovation efforts will yield a market advantage on consulting services for bleeding-edge technologies and corresponding performance optimisation since they've been through the problems their clients will face in the future.

This work stems from previous explorations with blockchain technologies, resulting in a corporate mobile application portal for partnership benefit claims such as shared expenses or loyalty programs. Crossjoin understood from this R&D effort that the organisation could start initiatives integrating shared client needs. This thesis proposal is part of a more comprehensive research program for an integrated platform for private and public asset management and transactions, which connects requirements and needs from one governmental client with a few private ones. The company's objective is to showcase the outcome of this specific initiative in tandem with other ongoing developments.

1.4 Document Structure

The rest of the document is structured as follows: In chapter 2 we provide an overview on most topics that are pertinent to the project and discuss relevant technologies that may be considered when developing the solution. Next, chapter 3 presents approaches and frameworks proposed by other authors, as well as government initiatives and solutions already available in the market that are relevant to the work. In chapter 4 we strictly define the scope that will be considered in the implementation phase and introduce the details of the planned solution, including its domain, design aspects, and specific technologies to be utilized. Finally, chapter 5 outlines the methods and criteria that will be used to evaluate the efficiency and effectiveness of the developed solution, and chapter 6 presents the proposed timeline for the implementation phase.

2

Background

2.1 Current State of Land Conveyancing

Real estate conveyance is by nature a process in which several intermediaries and authorities might be involved, and where different procedures and bureaucracies might take place depending on each country's legislation. This work will not target the system of any country in specific. Instead, we will try to generalize the land conveyance procedure and take only into consideration characteristics that are present in most of them. To achieve this, it is essential to firstly dive into a simplified view of the general flow of the process. This following section provides a summarized overview of the works done by Garcia-Teruel [21] and Shuaib et al. [43, 44].

The first step in a land deal is usually for the parties to hire **real estate agents** - professionals that help them find, buy, or sell a property and aid them during the transaction process. They provide guidance on market trends, property valuation, and legal requirements. Then, there must be an entity responsible for tasks such as verifying the identity of the transacting parties, preventing illegal activities and ensuring the legality and effectiveness of land transactions. In Western European countries, that entity is the **notary**. In Nordic countries, the whole process is actually completed by the real estate agents or by **lawyers**. England and Ireland have a system of **solicitors** or **licensed conveyancers** for this purpose. If we add mortgage loans to the mix, **Banks** are another entity to be involved, frequently along with lawyers and **property valuators**.
For a transaction to take place, several documents are required depending on jurisdiction. Examples include title deeds, bank statements, insurance proofs, energy certificates, government-issued permits, licenses relevant to the property, etc. These documents are often issued by various other entities and valuators. Additionally, pre-agreement contracts are often drafted before the final transaction. These documents serve as a formal declaration of intent and ensure that both parties are committed to the transaction. They outline the basic terms and conditions of the sale and may include clauses such as the price, payment schedule, and any conditions precedent to the sale. Once the transaction

has been completed, it shall be registered in the land registry by the competent authority, which could be a governmental authority, the courts, or an independent public authority. Table 2.1 describes a generic sequential flow of how a real estate transaction is usually processed, although exceptions may apply depending on each specific case [15, 44].

	Buyer	Seller
1.	Initiation through engagement of a real estate agent or lawyer	
2.	Mortgage loan due diligence (if applicable)	Sale legality verification and registration procedures
3.	Property visitation and negotiation phase	
4.	Drafting and signing of the letter of intent (pre-agreement contract)	
5.	Securing mortgage financing (if applicable) and gathering of necessary documentation	Gathering of required documentation
6.	Finalization of the sale agreement and execution of the financial transaction	
7.	Official recording of the transaction in the Land Registry by the designated authority	
8.	Handover of the keys	

Table 2.1: Steps in Land Conveyance

Rental Agreements, on the other hand, are generally simpler and less formal. They usually do not require the participation of intermediaries and are not even required to be registered in the land registry, although they shall be declared to authorities for taxation purposes. This lack of registration, however, creates opportunities for under-reporting of rental income leading to tax evasion.

2.2 Blockchain Overview

The term "blockchain" was initially popularized following the publication of the Bitcoin whitepaper in 2008 [31], by an anonymous author under the pseudonym of Satoshi Nakamoto. Although the term itself is not mentioned in the whitepaper, it began to be widely used to describe the underlying technology of Bitcoin. Since then, many other solutions have emerged utilizing similar or derived technologies, following the core principles of Bitcoin. Years of innovation and refinement have broadened the term's applicability, making it far more versatile than its original counterpart.
Blockchain is an innovative database technology that can be described as a digital and distributed ledger of transactions. These transactions are recorded in the form of blocks securely linked together via cryptographic hashes, effectively forming a chain, hence the name blockchain. Instead of relying on a centralized location managed by a single entity, blockchains are typically managed by a distributed Peer-to-Peer (P2P) computer network

composed of several nodes that can belong to different authorities who may not trust each other. This decentralized nature along with the following characteristics are what make blockchain so different from other database solutions [54]:

Consensus - For a new transaction to be recorded, it is required that most of the nodes in the network agree on its validity and inclusion.

Transparency - Transactions recorded on a blockchain are visible to all participants in the network, making it possible for anyone to verify the integrity of the ledger.

Immutability - Blockchain transactions are irreversible. Once a block has been recorded, all transactions it contains are executed and cannot be undone. In some cases, however, it is possible for them to be rollbacked.

Tamper-Resistance - Each block in the chain contains a cryptographic hash reference to the previous block, meaning that if a block were to be tampered with, all of the subsequent blocks would also need to be recalculated. Due to the consensus algorithmic security, this is an extremely difficult task.

Blockchains as we know today have grown to be much more than just an innovative way to store transactions, however. In some blockchains, such as Ethereum, any computable function may be implemented with Solidity, its Turing complete programming language for writing business logic. This allows blockchains not only to function as a way to store data and execute transactions but also as a way to implement an entire system's logic. These features have led many industries to explore blockchain's opportunities in business areas including Finance, Energy, Mobility, Smart Cities, IoT systems, and many more.

2.2.1 Public, Private and Consortium Blockchains

Blockchain ecosystems can be categorized based on network access as either public, private or consortium [54]. Public Blockchains are usually open and permissionless, meaning that anyone can set up a node and become part of the network by contributing to the ledger. This means that the content of the blockchain is fully visible to the public, and that every peer is equal and has the same set of roles and permissions. This is the most disruptive and innovative blockchain type, and therefore the most well-known. Bitcoin and Ethereum are the most popular examples. Public Blockchains are also closely associated with cryptocurrencies since there is a need to incentivize people to participate in the network. Each of these blockchains may have a native cryptocurrency token (e.g. Ether (ETH) for Ethereum, and Bitcoin (BTC) for Bitcoin) and by contributing to the ledger and behaving correctly, nodes are rewarded with a certain amount of that cryptocurrency. The way these tokens are generated has to do with the consensus algorithm being used. The two most common public blockchain consensus algorithms are the Proof-of-Work (PoW) and Proof-of-Stake (PoS), although there are many more.

In contrast, Private Blockchains are fundamentally different in their structure and purpose. These blockchains are closed and permissioned, meaning access to participate in the network is restricted to a pre-selected group of entities. This controlled access ensures that on-chain data remains within the trusted group, making private blockchains ideal for industries that deal with confidential data, like finance, healthcare, and real estate. Because in these networks the number of nodes is small in comparison to those of public blockchains, the consensus mechanisms are also quite different. Since there is no need to incentivize random people to participate in the network, there is no need to have a native cryptocurrency system. Without the need for cryptocurrency mining, private blockchains may use more efficient consensus algorithms like Byzantine Fault Tolerance (BFT) or Crash Fault Tolerance (CFT). These algorithms are designed to be efficient and reliable in smaller networks where the peers are known and trusted, resulting in faster transaction speeds and much lower processing costs compared to public blockchains.

Permissioned networks that are managed by various organizations, instead of by only one, are commonly referred to as Consortium Blockchains [53]. This model is beneficial when multiple organizations need to collaborate and share data securely without fully trusting each other. Consortium blockchains typically provide ways to define roles and permissions for each of the network's peers, thus facilitating controlled access and activity based on predefined rules and criteria. For this reason, it is often stated that consortium blockchains provide a middle ground between public and private blockchains, as they combine the transparency and collaborative aspects of public blockchains with the enhanced security and control found in private blockchains. Table 2.2 was originally proposed by Dib et al. [16] and highlights the technical differences between each of the discussed blockchain types.

Property	Blockchain Governance		
	Public	Consortium	Private
Governance Type	Consensus is public	Consensus by a set of participants	Consensus by a single owner
Transactions Validation	Anynode (or miner)	A list of authorized nodes (or validators)	
Consensus Algorithm	Without permission (PoW, PoS, PoET, etc.)	With permission (PBFT, Tendermint, PoA, etc.)	
Transactions Reading	Any node	Any node (without permission) or A list of predefined nodes (with permission)	
Data Immutability	Yes, rollback is almost impossible	Yes, but blockchain rollback is possible	
Transactions Throughput	Low (few dozen per second)	High (hundreds/thousands transactions per second)	
Network scalability	High	Low to medium (a few dozen/hundred of nodes)	
Infrastructure	Highly-Decentralized	Decentralized	Distributed
Features	Censorship resistance Unregulated and cross-borders Support of native assets Anonymous identities Scalable network architecture	Applicable to highly regulated business Efficient transactions throughput Transactions without fees Infrastructure rules are easier to manage Better protection against external disturbances	
Technologies	Bitcoin, Ethereum, Ripple, etc.	MultiChain, Quorum, HyperLedger, etc.	

Table 2.2: Blockchain Classification. Source: Adapted from [16]

2.3 Public Key Infrastructure (PKI)

Beyond the peer nodes, responsible for maintaining the blockchain's ledger and validating transactions, other participants interact with the blockchain, such as end users and client applications. These are the individuals who use the system for its intended purposes and submit transactions to be validated by the nodes. Each of these is uniquely identified by a cryptographic key pair, which consists of a public and a private key. These key pairs are the foundation of blockchain's security guarantees, as they ensure transaction authenticity and integrity. As the name suggests, the public key is made public and may be openly shared. It may be used by others in the network to encrypt messages that only the holder of the corresponding private key can decrypt. Within the context of a blockchain network, it primarily serves as a user's identifier or address. The private key, however, is secret and should only be known by the user, as it serves to digitally sign transactions in its name. Others may verify this signature using the corresponding public key. Public and private keys are intrinsically linked as the public key is generated by the private key itself. However, due to the cryptographic nature of the key pair, it is not feasible to derive the private key from the public key [46]. Finally, each public key is authenticated and validated through a public key certificate, a digital certification provided and issued by a Certificate Authority (CA), which confirms the legitimacy and trustworthiness of the public key. X.509 is the standard format for public key certificates, widely used in various secure internet protocols. Public Key Infrastructure (PKI) is commonly defined as the set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates.

In public blockchains, the management of the key pairs is at the responsibility of the individual users. The network itself provides PKI support, enabling signature verification across different independent nodes. However, the public key is the only known information about the user, meaning that each account is intrinsically anonym. Because of this, it is very complex to establish a one-to-one relationship of key pairs to real-world identities, as a user may create many key pairs. In some cases where it is possible, these connections are typically made through processes outside, and not explicitly supported by the blockchain itself [53]. In contrast, permissioned blockchains might have a more centralized approach to PKI, with designated authorities responsible for issuing and managing the key pairs. This centralized approach makes private networks best suited for scenarios where the generation of key pairs must be regulated and makes it easier to connect them to real-world entities. They can offer other advantages such as facilitating user authentication through conventional methods like usernames and passwords, and provide additional recovery options in case of lost credentials.

2.4 Smart Contracts

In 1994, Nick Szabo first defined a smart contract as a "computerized transaction protocol that executes the terms of a contract" [48], being a contract an agreement that can be enforced by law. While the core concept remains the same, the smart contracts that we know today refer to code deployed in blockchain networks, that comprise any programming logic and may perform transactions autonomously. Not every blockchain infrastructure supports smart contract deployment, and for the ones that do, the programming language used to define their logic may differ. Ethereum, for instance, uses Solidity, a programming language created specifically for smart contract implementation. In private blockchain development, it is common for frameworks to allow smart contract specification using general-purpose programming languages such as Python, Java, and Javascript. According to the blockchain properties previously discussed, smart contracts are immutable once deployed, meaning the contract cannot be changed or broken, ensuring a high level of security and trustworthiness. They may act as transaction escrows, removing the need for additional intermediaries. Smart contracts are a foundational component of many blockchain platforms and are essential in the creation of Decentralized Applications (dApps).

2.5 Tokenization

One of smart contracts' most important capabilities is their ability to create and manage digital assets that we name blockchain tokens. Overall, tokens are more of a public blockchain concept, as most of permissioned blockchain frameworks don't support direct token standards or libraries. However, there may be times when it may make sense to replicate their logic in private networks, depending on the system requirements. Tokens have an owner, but their ownership might change. They can be classified into fungible or non-fungible, based on their interchangeability [20].

Fungible Tokens refer to tokens whose units are equal and interchangeable with each other since they hold the same value and properties. This means that one unit of a fungible token can be exchanged on a one-to-one basis with any other unit of the same token type, as they have equal value. Ownership over this kind of token can be seen as "how many units of X token does user Y have?". They may also be divisible into smaller units. By this definition, cryptocurrencies themselves like BTC and ETH are fungible tokens. However, they can be used for a variety of other things, such as representing points in a ranking system, voting rights, or even shares over an asset. In Ethereum, ERC-20 is the most popular standard for fungible token definition.

Non-fungible Tokens (NFTs), on the other hand, are unique and cannot be exchanged on a one-to-one basis with each other, although they can still be traded and exchanged for money, cryptocurrencies, or other NFTs. Each NFT is indivisible and has its own value and properties. They are used to represent ownership and proof of authenticity of a unique digital item, such as digital art and collectibles. These tokens are created through a process called minting, usually initiated through a mint function defined in the NFT smart contract, in which the information such as its owner and its metadata are provided. After this information is validated by the network, a block comprising the NFT is submitted on the blockchain, and the NFT is minted. Ethereum was the first and is currently the most popular blockchain for NFTs, being ERC-721 the most common standard for non-fungible token definition. However, many other notable blockchains have already adopted the concept.

Although tokens are fundamentally digital assets, they can act as a digital representation of a real-world physical asset. "Tokenization" is the process of converting rights of an asset into a digital token on a blockchain network. To these tokens we call Security Tokens [14]. There are multiple advantages that justify why someone would want to tokenize an asset. One of them is to increase the liquidity of assets that are traditionally illiquid or hard to transfer, such as real estate or company shares. By creating digital tokens, these assets can be easily traded on digital platforms since systems can be developed to simplify the exchange process and remove intermediaries. Another advantage is the ability to divide the asset into smaller parts, allowing for fractional ownership. Finally, by keeping the asset ownership recorded on a blockchain, it becomes possible to view the complete history of ownership, enhancing transparency and trust in the transaction process. Tokenizing an asset is not a trivial process, however. Security tokens must often comply with various regulatory frameworks depending on the jurisdiction. The U.S. treats security tokens similarly to traditional securities, applying existing securities laws through the Securities and Exchange Commission (SEC). The EU has been working on creating a comprehensive framework for digital assets, including security tokens, through the Markets in Crypto-Assets (MiCA) regulation [19], which entered into force in June 2023. This is a very hot topic with a lot of research going on in recent years, which reflects the growing importance of digital assets in the financial industry. The ERC-1400 was the first and until very recently the only Ethereum standard for security tokens. In December 2023, T-REX Protocol [49] achieved 'final' status and was recognized as the ERC-3643 security token standard. These standards use different approaches, but both of them focus on enabling the enforcement of compliance rules and the control of transfers to eligible investors.

2.6 IPFS

The InterPlanetary File System (IPFS) [6] is an open-source protocol and peer-to-peer network for storing and sharing data in a distributed file system. It functions similarly to a framework and can be utilized for implementing decentralized data storage solutions. By default, IPFS operates as a public, open network where anyone can participate by running a node. However, it is possible to create private IPFS networks where access is restricted, making it also useful for enterprise applications or private consortiums where data privacy is a priority. Although IPFS itself is not a blockchain, it complements blockchain technology really well. One of the biggest limitations of blockchain is its data storage capabilities. Since every node must run a copy of the entire ledger, it would be unreasonable to store large amounts of data on-chain. Although this problem is more relevant in public blockchain networks, due to bandwidth limitations and high transaction costs, it is still present in private networks that require storing large amounts of data. For this reason, IPFS is a very popular solution for off-chain storage in both public and private blockchain environments. It's designed to enhance data availability and redundancy while preserving the decentralized nature of the system.

2.7 Development Frameworks

The development framework is the tool that will allow us to code the business logic and specify the network characteristics regarding the peers and their roles. In this section we present an overview of the different frameworks available for developing permissioned blockchain networks.

2.7.1 R3 Corda

Corda [10] is an open-source permissioned blockchain platform developed by R3. It is particularly suited for finance-related applications as it has a strong focus on facilitating legal processes. One of its great features is its enhanced interoperability, as the platform is able to seamlessly interact and integrate with various systems and networks. CorDapps, Corda's solution for implementing business logic, supports development both in Kotlin and Java. They are significantly different from smart contracts as they are more structured and designed to be legally enforceable.

2.7.2 ConsenSys Quorum

Quorum [13] is a permissioned blockchain framework that enables enterprises to leverage Ethereum for their private blockchain applications. It utilizes a modified version of Ethereum's blockchain protocol, keeping its core technology such as its runtime environment (EVM) and solidity smart contracts, but supports private consensus algorithms like Raft and other permissioned network capabilities. This allows solutions to benefit from the robust development tools and testing environments that Ethereum offers while keeping them completely independent from Ethereum's public network.

2.7.3 Multichain

Multichain [23] is an open-source permissioned blockchain platform that stands out for its ease of use and quick deployment. It distinguishes itself through its compatibility with a wide range of programming languages, which enhances its interoperability across various systems and networks. However, Multichain may not be the optimal choice for applications requiring complex business logic development, as it is designed for simpler blockchain implementations.

2.7.4 Algorand

Algorand [12] is primarily recognized as a public, decentralized blockchain network, but it also offers capabilities for deploying permissioned networks. The code for Algorand is open-source so it can be cloned and used in private blockchains. Algorand supports the creation and management of tokens and smart contracts, and utilizes a unique consensus mechanism called Pure Proof of Stake (PPoS), which enables the network to handle high transaction throughput with minimal fees.

2.7.5 Hyperledger Fabric

Hyperledger Fabric [25] is an open-source permissioned distributed ledger technology hosted by the Linux Foundation. It is best known for its high flexibility and modularity, as it allows network designers to seamlessly plug in their preferred components like consensus and membership services. Fabric follows a smart contract-like architecture for implementing the business logic, commonly referred to as chaincode. They offer support for developing chaincode in various programming languages such as Go, Javascript, and even Solidity through the use of Hyperledger Burrow.

2.7.5.1 Peers

A network in Hyperledger Fabric is established by multiple organizations that may consolidate different kinds of peer nodes, along with an endorsement policy defining which or how many of them must validate a transaction before it is appended to the chain.

Endorsing Peers - The peers to which clients send transaction requests. They simulate the transaction execution on isolated containers. Based on that simulation, they decide whether the transaction is valid or not. If it is, they send the endorsed (signed) transaction back to the client, which in turn sends it to the ordering peers.

Ordering Peers - Also referred to as the Ordering Service, these peers verify all the endorsed transactions and assemble them into ordered blocks to be appended to the ledger, further sending them to the committing peers. It's between these peers that the consensus mechanism takes place.

Committing Peers - The committing peers are every peer that keeps the current state of the ledger. Once they receive a new block from the ordering service, they validate the transactions once again, and then append the block to the ledger. Transactions that fail this validation are still recorded but marked as invalid. The concept of committing peers is usually abstracted as it is common for every peer in the network to be a committing peer.

Anchor Peers - Each organization must delegate one or more anchor peers that serve as intermediaries between peers from their organization and peers from other organizations. These are the peers that all other peers can discover and communicate with using the Gossip protocol.

It is important to note that these terms are not mutually exclusive, meaning a single node may be a peer of various kinds. In fact, a single node could be a peer of every kind. However, due to security reasons, this is generally not advisable. The ordering service should not be part of the same organization as the endorsing peers, as this could introduce centralization and a single point of failure. Figure 2.1 illustrates the transaction flow in Hyperledger Fabric through a sequence diagram.

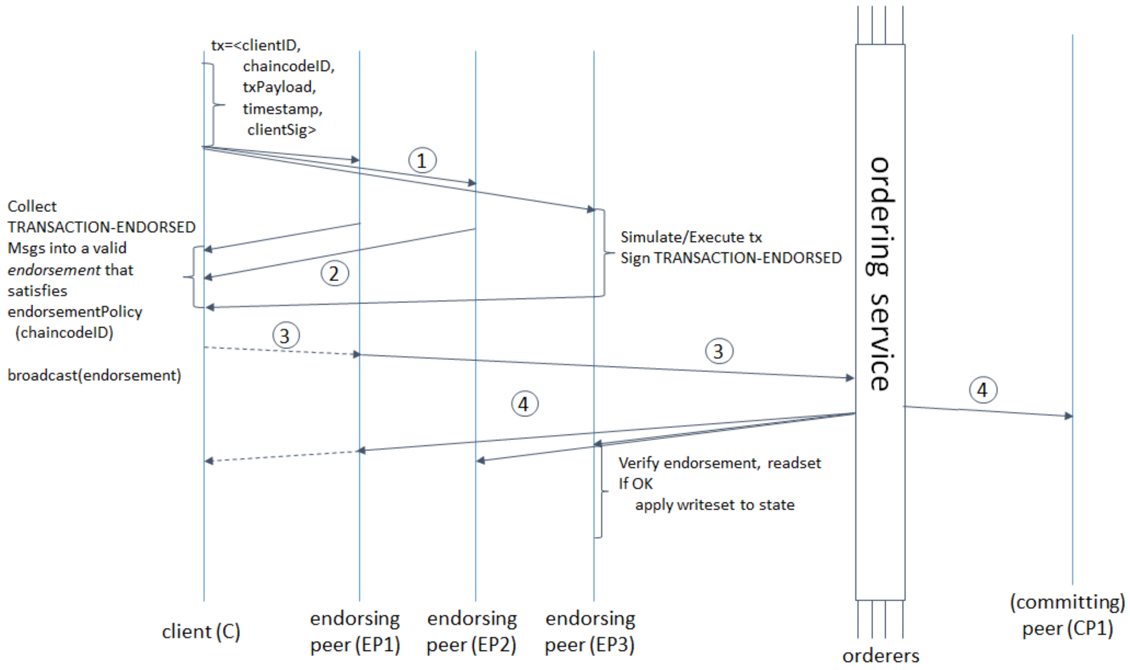

Figure 2.1: Hyperledger Fabric Transaction Flow. Source: [26]

2.7.5.2 Channels

Furthermore, for each organization, it is possible to configure different permissions regarding what kind of data it may read and modify. Fabric achieves that through the concept of channels. An important aspect to understand is that in a Fabric network, there may be more than one independent ledger. A channel in Hyperledger Fabric is a private "subnet" of communication between any number of network members, for the purpose of conducting private and confidential transactions [26]. Each channel has its own independent ledger and chaincode, so the state and transaction history of one channel are only visible to the members of that channel. So instead of having a single ledger shared by the entire network, in Fabric we may have multiple channels for various purposes and business processes. There may or may not be a channel to which every organization has access.

2.7.5.3 MSP

Hyperledger Fabric uses PKI to verify the actions of all network participants. Every node, network administrator, and user submitting transactions need to have a public certificate and private key to verify their identity [26]. Since Fabric is a permissioned network, there's a need to delegate an authority (or multiple authorities) to provide the PKI over the network. Membership Service Provider (MSP) is a layer built on top of PKI and Fabric's abstraction of network membership architecture. It manages identities through public key certificates, allowing CAs to identify and authenticate the network participants. Then, it turns those identities into roles by identifying specific privileges and permissions for reading and writing data on the different channels, thus playing a crucial role in access control. For instance, if a peer uses its private key to digitally sign a transaction, the MSP is used to check whether the peer is allowed to endorse the transaction. Moreover, it is decentralized in the sense that it is possible and recommended to have different MSPs represent different organizations. For instance, each organization participating in a Fabric network may have its own MSP, ensuring that each member's identity is unique and authenticated within their own organization. In practice, the implementation of the MSP is just a set of folders that are added to the configuration of the network that define which Root CA and Intermediate CAs are accepted to define the members of a trust domain [26].

2.8 Framework Comparison

We now present a side-to-side comparison of the previously presented frameworks, regarding the following aspects that we found relevant to the scope of the project:

Programming Language - The programming language used to code the logic differs from framework to framework. There's not a single best language for this purpose, so if various options are available, the choice is usually made by the developer.

Solidity Compatibility - Even if Solidity is not the main programming language, some frameworks provide support for writing code using Solidity.

Smart Contracts - Not all of the presented frameworks use the concept of smart contracts. R3 Corda, for instance, uses CorDapps that function in a different way to traditional smart contract architecture.

Native Token Support - The concept of tokens is generally more associated with public blockchains, mainly Ethereum. Some frameworks, however, provide ways of natively implementing tokens similar to those of Ethereum, using libraries or built-in functionalities. For those that do not have native token support, we would need to implement the tokens from scratch.

Access Permissioning - One of the most important aspects when designing a consortium blockchain is defining peers' and participants' roles and permissions.

Time-based Event Support - If the framework provides ways of implementing smart contracts or functions that autonomously trigger based on a time event. This could be useful, for instance, to implement recurring transactions of rent payment, triggered each month.

Community Support - If the framework has continuous community support, regular updates, comprehensive documentation, and good online resources.

Development Tools - If the framework provides robust development tools and comprehensive ways of testing the solution.

Complexity - Since the developed solution is essentially a Proof-of-Concept, and the time frame is not the largest, the overall complexity and learning curve associated with each framework represents a significant factor.

Table 2.3 summarizes the considered characteristics of each of the frameworks analyzed.

Framework	**Hyperledger Fabric**	**R3 Corda**	**Quorum**	**Multichain**	**Algorand**
Progr. Language	Golang	Java, Kotlin	Solidity	Many	Python
Solidity Compatibility	Yes	No	Yes	No	No
Smart Contracts	Yes (Chaincode)	No (CorDapps)	Yes (Ethereum)	No	Yes (ASC1)
Native Token Support	No*	Yes (SDKs)	Yes	Simple	Yes (ASA)
Access Permissioning	Strong (RBAC)	Strong (RBAC)	Simple	Strong	Simple
Time-based Event Support	No	Yes	No	No	No
Community Support	Strong	Strong	Lacking	Good	Good
Development Tools	Robust	Robust	Comprehensive	Solid	Solid
Complexity	Complex	Moderate	Simple	Simple	Moderate

Table 2.3: Comparison of Blockchain Frameworks

* Not natively supported, but implementable through chaincode.

3

Related Work

A very valid question that may come up is "Why Blockchain? Can't we just use any other technology we already know?" Blockchain technology may neither be the only nor the best solution to this problem. But there are many reasons why it looks like one of the best contenders. As previously explained, blockchain can provide not only a shared database but also ways to deploy code and build entire applications. This can be used to automate the process of land conveyance, renting, mortgage loans, and much more. In a utopian scenario, all operations related to real estate could be executed over a blockchain infrastructure. Many of these processes that are originally manual and require efforts from every party involved could be fully automated and done remotely through smart contracts and digital signatures. The smart contracts would execute the business flow without the opportunity to be manipulated, thus reducing corruption and fraud. Furthermore, blockchain may bring opportunities that cannot be achieved in the current infrastructure. It would maintain a complete and transparent history of details regarding every deal made concerning each property, improving the search process and helping in the decision-making for buying and renting real estate. By removing intermediaries and unnecessary steps, it could greatly decrease the overall cost of the process. Moreover, it would bring new and improved ways to invest in the real estate market, as tokenizing real estate assets highly increases liquidity and allows fractional ownership. Some of these opportunities are discussed in greater detail in the following sections, as we present related work done by other authors, companies, and governments.

3.1 Fractional Ownership of Assets

A topic that is frequently discussed among many authors is how to represent fractional ownership of assets in blockchain platforms. As previously explained, in public blockchains, assets such as real estate properties are frequently represented through Non-fungible Tokens (NFTs). However, a challenge arises as NFTs only support single ownership, meaning a single token can only belong to a single owner. There are a few ways to circumvent this. One method involves using fungible tokens such as ERC-20 tokens to represent ownership shares in an asset. For instance, a single real estate property can be represented by a fixed number of ERC-20 tokens, with each token representing an equal share of the property. Gupta et al. [24] considered using ERC-777, another standard for fungible tokens with added features, in the same way. A hybrid model can also be considered, combining features of both NFTs and fungible tokens. The real estate asset may be represented through an NFT for uniqueness, and then linking this NFT to fungible tokens that represent fractional ownership shares. Joshi et al. [27] suggested implementing this approach by using the ERC-1155 multi-token standard for real estate tokenization. Unlike the previous standards, the ERC-1155 can mint both fungible and non-fungible tokens, eliminating the complexity of handling two token standards and their interaction. In the proposed model, each property is associated with a unique NFT and fungible token type within the ERC-1155 contract. Owning a share of the fungible tokens minted for a property equals owning a fraction of that property.

Most private blockchains do not inherently support tokens similar to those of Ethereum, as it wouldn't make sense since ERC tokens are adapted to Ethereum characteristics. However, it is relevant to discuss them as it is still possible to replicate their logic, or at least take some aspects of their architecture and functionality as inspiration.

3.2 Rental Opportunities

The real estate rental market is another sector in need of innovation and improvement, afflicted by inefficiencies and a significant presence of informal transactions that should be regulated. The process of long-term rentals still results in frustration and lost time for both the owners and potential tenants. There has not yet been technological disruption significant enough to conduct a new and better way to rent [37]. If we were to have a unified blockchain-based registry for real estate properties, the next logical step would be to facilitate the rental process by digitizing rent contracts through smart contracts. Blockchain and smart contracts might allow for automatic recurring payments, contract registration, and automatic payment of taxes, thus being an opportunity to promote the registration of rental agreements while reducing the black market [21]. It would bring several advantages to the landlord as the tenant's relevant background data such as rental history, credit rating, and reviews could be made visible and aid in the decision-making of signing a rental agreement.

Karamitsos et al. [28] conceptualized an Ethereum smart contract architecture for a real estate renting system. Only two entities were taken into consideration - contract owners (representing landlords) and users responsible for creating Ethereum wallets (representing tenants). The smart contracts serve as a way to establish a rental agreement between these two entities - the landlord initiates a contract by setting up the rental terms, and the contract is started as soon as a tenant signs it, meaning a rental agreement is formed. The tenant is then responsible for depositing funds in the smart contract through the payment function, which automatically sends the funds to the landlord. The contract also supports a termination function, in which the security deposit is sent back to the tenants.

3.3 Investment Opportunities

The opportunities that Blockchain may bring to the real estate sector can even reach the investment world. Real Estate investment is at the same time one of the safest and the most challenging forms of investing. This mostly has to do with the initial investment required to purchase property, and with the fact that real estate is notoriously difficult to liquidate, due to the insane amount of underlying bureaucracies, mediators, and fees [27]. More complications are added if we think about partitioning a property into smaller fractions. A blockchain-based approach could potentially lift these challenges, however. Smart contract procedures could automate and simplify the exchange process and remove intermediaries. Through tokenization, these assets can be easily divided into smaller parts, allowing for fractional ownership.

Gupta et al. [24] described a workflow for tokenizing real estate within a public blockchain network, that allows for a more efficient and accessible way of real estate investment. This tokenization mechanism consists of a "legal trick" in which an intermediate business entity is used to indirectly tokenize a real estate asset. These business entities can be something like a Special Purpose Vehicle (SPV) or a Limited Liability Company (LLC) which are legal entities that have certain characteristics of a company, with their own assets, liabilities, and legal status. As such, they allow multiple investors to collectively acquire shares of it. By having a Special Purpose Vehicle own a single asset, the SPV can be sold itself, rather than attempting to split the asset between the various parties. The SPV would be tokenized and its shares would be distributed to the token holders. Buying a token would be equivalent to buying a share of the SPV that owns an asset, which in theory translates to acquiring a fraction of ownership over that asset [36]. This approach is currently one of the only reliable and legal ways to tokenize an asset and has been the means for most of the private companies to support ownership tokenization on their solutions, as we will discuss further ahead.

3.4 Developed Frameworks

As Saari et al. [39] verified in 2022 through an extensive literature survey, in the last few years the number of academic literature released about the potential uses of blockchain in the real estate industry has increased significantly. Still, very few of them present empirical evidence and practical examples of use cases.

Ali et al. [2] proposed a private permissioned blockchain smart contract architecture for land registration that would hypothetically replace Saudi Arabia's current infrastructure. The framework includes functionalities for facilitating the buying and selling process while providing a detailed transaction history and untampered information regarding a property. Being a private blockchain network, it would be managed by a central government authority that executes all types of contracts among the participants (buyers and land owners), with the participants responsible for submitting the required documents to complete the various operations. The network also includes other justice-related entities to help endorse the transactions, for instance by validating all the documents related to them. X.509 certificates and keys are generated for the various participants and the administrator of the network, and ideally a governmental entity would verify the keys and relate them to the identity of a citizen. The authors indicate that a proof of concept was implemented using Hyperledger Fabric, however, the code was not made available.

Sen et al. [40] also proposed a smart contract-based permissioned blockchain framework in Hyperledger Fabric, for the Electronic Property Registration domain of e-Governance in India. The solution considered a set of peer organizations such as a Registration Authority (the one handling the MSP), a Land Authority and a Municipal Authority, and participants such as the seller, the buyer, mortgage agencies, and insurance agencies. The main objective was to ensure secure storage of the records by defining access rules for the various stakeholders. For this, the solution comprised the definition of three different channels with dedicated smart contracts - the first focused on property transactions, another for querying information and providing verification services to the involved agencies, and a final one exclusively dedicated to the private transactions between the three government organizations (the peers).

Alam et al. [1] proposed a three-phased blockchain-based strategy to modernize Bangladesh's inefficient and outdated land registry system. The current system relies heavily on physical documents managed by various authorities, leading to long and cumbersome processes susceptible to corruption and bribery. The authors recognize that one of the biggest challenges for the initial adoption of a blockchain system for managing title registry is to establish the necessary infrastructure. And so, for the first phase, a public blockchain network is proposed. The process would still be overseen by a government entity, however, regular people would be capable of being miners, thus alleviating the burden of rapidly constructing a comprehensive infrastructure. This first phase would only work as a timestamp logger of ongoing land handovers, ownership transfers, or financing events since it wouldn't be reasonable to think about moving all existing land records to the Blockchain system in an initial phase. The second phase introduces a small-scale hybrid blockchain network. Here, selected organizations equipped with high-capacity nodes would act as miners, and a private blockchain ledger would gradually incorporate the public blockchain data. This phase also incorporates multi-party PKI-based trusted communication for the involved parties and requires users to contact a Certificate Authority for public-private key pairs. The final phase is a full hybrid blockchain network, where even more public and private institutes with high computing capacities get involved in the mining process, and all documents are digitized and stored in a distributed file system like IPFS. Finally, a smart contract architecture illustrating the first phase is presented through an Unified Modeling Language (UML) Class Diagram, in which fractional ownership is supported, and includes functionalities for user creation, land registration, and assigning ownership.

3.5 Governmental Initiatives

Many governments have already shown interest in exploring what kind of opportunities blockchain technology could bring to real estate and land registration. We now present an overview of Proofs-of-Concept (PoCs) and Testbeds done worldwide in recent years.

3.5.1 Sweden

In the recent past, Sweden has tested applications for blockchain technology in their land registry system. The 2017 proof-of-concept refined and tested a blockchain-based solution for handling real estate transactions, to analyze the potential benefits of using smart contracts for land conveyance and mitigating existing problems mostly related to complexity, duration, duplication, and documents being physical, without the need for significant land agency disruption, complete IT infrastructure rebuilds, or full database redesign [7, 29]. The project was sponsored by a variety of entities such as ChromaWay (technology provider), Kairos Future (business), Telia (ID Provider), SBAB Bank, and Landshypotek (bank). The proposed solution consisted of a permissioned private blockchain network managed by either public or private entities, each with its conditions and authorizations. All the digital files relative to the ownership of land, mortgage deeds, and transaction processes are stored off-chain, while the blockchain network keeps an audit trail and handles the authenticity, the signatures, and the integrity of the whole process, by storing cryptographic hashes of the referred files. The solution took advantage of ChromaWay's Esplix technology - a system for exchanging signed messages - and their Postchain framework - an open-source relational blockchain solution - for the development of the consortium blockchain, as well as Telia's digital ID solution to handle user registration. Although the idea was for the Swedish Lantmäteriet (The Swedish Mapping, Cadastre, and Land Registration Authority) to store the blockchain with the proofs, the blockchain would also be stored and validated by other actors such as banks, real estate agents, buyers, and sellers. The results of the proof-of-concept could be seen in faster transactions, the development of a fully digital process, greater transparency for all parties, increased security, better redundancy of data, and the elimination of physical storage and other paper-based work such as traditional mail. The number of manual steps needed for a property transaction saw a dramatic decrease from 34 to just 13. Significant improvements were also pointed out in the process of mortgage deeds. From these takes, we can see that the project was a great success from the result point of view, however it ended up not being implemented. The reason for that lies in the fact that the Sweden law still does not allow for the use of electronic signatures for property transactions, and so further progress is expected once the digital signature restrictions are addressed [7].

Beyond the Swedish case, ChromaWay has also supported a few other initiatives in other legislations. Examples of those are the PoCs developed for Australia and Canada - both also hybrid solutions, but unlike the Swedish case, which focused on the complete case of land conveyance, these projects are focused on more specific land administration processes [7]. The Australian case focused on the “Discharge of Mortgage Lien”, which allegedly was an overly complicated process that included more steps than necessary, while the Canadian case focused on "Re-Assignment Reporting”.

3.5.2 Georgia

Disrupting the legacy systems becomes even more valuable in developing countries without a reliable track record of real estate ownership and land registry, where corruption might dominate and the integrity of official documents could be questionable. Projects of this kind may be the simplest and most efficient way to increase Gross Domestic Product (GDP) in the medium term [21].

Georgia’s land registration and transaction process was infamous for being long and prone to corruption. Even so, its reputation has been changing drastically, as the government has been devoted to modernizing its systems. In 2016, it was announced that a collaboration between the government of Georgia and BitFury - an American provider of Bitcoin blockchain infrastructure - had taken place, aiming to design and pilot a private permissioned blockchain operated by the National Agency of Public Registry (NAPR) and anchored to the Bitcoin Blockchain through a distributed digital time-stamping service [41]. The pilot was a success and so, later in 2017, the system was expanded, allowing blockchain technology to facilitate the purchase and sale of land, reducing the transaction costs to about 0.1% of the property value [42, 44]. The project has been completed and made available to the public, making the Republic of Georgia the first government to use blockchain technology to store and validate land registry information. Following the constant updates and renovations, Georgia ranked fifth in the world for ease of registering a property, according to The World Bank Doing Business Report, in 2019 [51].

3.5.3 Estonia

Estonia has been proud to be a model to follow when it comes to promoting research in new technologies to reform traditional systems. It is a country where almost every bureaucratic task can be done online and when it comes to blockchain, titles itself as the #1 Country to use blockchain on a national level. In fact, Estonia had already started research on blockchain technology in 2008 – even before the release of the Bitcoin whitepaper, that first coined the term "blockchain" [17]. As of today, Estonia uses the KSI blockchain technology [18] to secure the integrity of government data and systems. That includes protection over services ranging from health records, law and court systems, banking, and, of course, land registry. While not the utopian scenario, it is stated that 'millions of lives and resources are saved as the potential manipulation of defense data or smart war machines is prevented using blockchain technology'.

3.5.4 Brazil

In 2016, company Ubiquity partnered with the Brazilian land registry, "Cartório de Registro de Imóveis" with the goal of developing a blockchain-based title registry pilot project. The project aimed to achieve completely paperless and transparent land transactions and registrations. Initially, the project started with a parallel system alongside the existing land registry, before fully transitioning to blockchain. The developed implementation was tested in two Brazilian municipalities, Pelotas and Morro Redondo [5].

3.5.5 Honduras

Honduras is another case of a developing country trying to improve its land registration system through blockchain technology. This one, however, ended up not succeeding. The land registration system in Honduras faces significant challenges and inefficiencies. Title fraud and corruption are usual, ownership information is not properly recorded and is easily tampered with. According to USAID in a 2018 estimate, only 14% of Hondurans legally occupy properties [50]. In 2015, the government of Honduras reached out to Factom - an American blockchain technology company - to discuss the possibility of developing a new system for land registry. Factom proposed a blockchain-based solution layer to maintain a permanent, timestamped record of a land transfer on top of Bitcoin's blockchain [11]. By this time, numerous press reports could be found about this initiative, however, the Honduran Government never made any public comments about it, and no further developments were ever known. In 2018, Castellanos et al. [11] conducted an interview with the liaison between Factom and the Honduran government, to further investigate the status of the project. From the interviews, it was learned that there were several difficulties imposed by the government, some of which were related to the project happening near an election cycle, leaving government officials reluctant to introduce any major changes that could be used as a threat to the sitting government. The project was halted in mid-2017 due to the impending presidential elections and has not been reactivated since then [11].

3.6 Commercial Solutions

3.6.1 Propy

In recent years, Propy has caused an uproar, announcing to conduct “the first real estate transaction ever sold and transferred on the blockchain” [33]. This accomplishment is certainly impressive, however, there’s a slight catch. Propy’s mission is in fact for government bodies to recognize its registry as the official ledger of record such that property transactions made on the Propy platform are acknowledged as legal transfer of the property ownership. But as of right now, it mostly functions as a platform that complements and integrates with existing land registry systems. Propy’s platform allows for the digital upload and signing of traditional documents such as real estate ownership agreements and mortgage deeds [34]. This simplifies and eases the process of a real estate transaction since the process can be done mainly digitally, saving hours for everyone involved in the transaction. All the traditional paperwork is still on board, so this platform does not replace lawyers or intermediaries but instead provides them with tools to facilitate document sharing and signing, notifying all parties involved. Additionally, Propy provides multiple ways to carry out the transaction itself, whether from a traditional deal, from using cryptocurrencies, or by tokenizing a real estate asset and auctioning it. To make this possible, Propy mirrors government records in its blockchain network built on top of Ethereum and uses IPFS to store all the required files and documents. PRO tokens act as the main currency for crypto transactions and are built on top of the ERC-20 standard for Ethereum fungible tokens. Tokenized Real Estate properties are represented by a Propy-developed NFT which is allegedly capable of tokenizing any property in the United States. Transferring the possession of this NFT acts as a proxy for the purchase of the real estate since Propy has developed proprietary legal paperwork to encapsulate property rights into a US-based legislation entity [34]. Finally, Propy’s smart contracts act as payment escrows in the transaction. So going back to the first statement, it wouldn’t be fair to say that the real estate property was entirely sold via blockchain, but instead that a blockchain platform was used to facilitate the traditional transaction process.

3.6.2 RealT and Binaryx

RealT and Binaryx are both companies that take advantage of the previously mentioned approach described by Gupta et al. [24] - the use of intermediate legal entities in order to indirectly tokenize a real estate asset. This “legal trick” comes down to creating a business entity such as an SPV or an LLC for each real estate property, and legally assigning it as the property’s owner. Then, fungible tokens are created each representing a share of that business entity (“RealTokens” for RealT [36] and “bAsset tokens” for Binaryx [9]), which can be bought and sold through their marketplace platform. Buying a token of a real estate property is equivalent to buying a share of the business entity that owns that property, which in theory translates to acquiring a fraction of ownership over the asset [36]. But in practice, it is the business entity that is being tokenized, and not the actual underlying asset [24]. This means that RealT and Binaryx essentially provide an investment platform for real estate, where investors can purchase fractional shares for as little as US$50. This approach effectively removes the primary obstacle to entering the real estate investment market, which is the high cost of entry. As to property management, since a property listed on these platforms can grow to have thousands of owners, it is unrealistic to expect all of them to coordinate proper management decisions. Instead, RealT and Binaryx offer services to upkeep the property and manage all landlord responsibilities, while the token holders only have to worry about voting for basic operations like raising or lowering the rent cost [9, 36]. This is usually done through a Decentralized Autonomous Organization (DAO) implemented with smart contracts. RealT's system architecture is built on top of Ethereum, and the RealTokens are a branch of the ERC-20 standard for digital tokens. Dai stablecoin is used to distribute rental incomes to the RealToken holders, ensuring that these are not subject to the volatility often associated with other cryptocurrencies. IPFS is also used to provide all RealToken owners with access to their relevant documents [36]. The implementation details of Binaryx are still not publicly available since the company is still at an early stage.

There are other companies that proposed similar approaches to RealT and Binaryx. Laprop [30] is a recent one, however, there is still not much to be found about it other than the first whitepaper released in 2022. REX Protocol [38] is another initiative that appeared in the same time period, and similar to Laprop, no recent developments were found. Atlant was one of the most promising initiatives in 2017 [4], but information regarding the project seems to have stopped, so it is likely that it failed.

3.6.3 Rentberry

The rental market is also already being explored by companies like Rentberry, which describes itself as a "decentralized long-term rental ecosystem that uses blockchain technology to make the rental process less costly and more convenient and secure" [37]. Rentberry's platform can be used to complete most rental tasks like searching for properties, making offers/bids, negotiating terms, e-signing contracts, and paying rent. The platform runs on top of Ethereum, and its transactions are made using BERRY tokens (a variant of ERC-20) as the currency, which can be used for a variety of other services like property promotion and marketing or hiring third-party service providers, such as house cleaners, handymen, plumbers, electricians, etc. The platform is already fully operational and accessible to the public via their website. Rentberry serves as a good example of how there is room for improvement in the current rental process, and how blockchain technology could help overcome many of its current challenges.

4

Proposed Work

Many of the solutions presented in the previous chapter are hybrid approaches in the sense that they propose to keep the legacy land registration infrastructure as is and aim to complement it in some way by using blockchain technology. They deliver the benefits of smart contracts whilst minimizing risk and resistance by ensuring minimal disruption. These approaches are very valuable and are the most likely to be implemented in the near future, as complete tokenization of property within any jurisdiction is probably still several years from becoming a reality [8].

The goal of this work is to imagine and conceptualize the architecture of a system that would rely on blockchain as the foundational infrastructure to store land registry data, by having the blockchain network replace the central database and store the actual records.

In this chapter, we introduce the details of the planned solution. Before delving into the specifics, however, it is important to define and discuss the scope in which this work will take place. Real Estate and land registry management is an immensely vast and complex field, with countless opportunities for deepening and expansion. It is thus unreasonable to consider the whole width of possibilities in a single study.

> Depending on the complexity of implementing the proposed system, it is possible that in the final version the scope might need to be adjusted or narrowed.

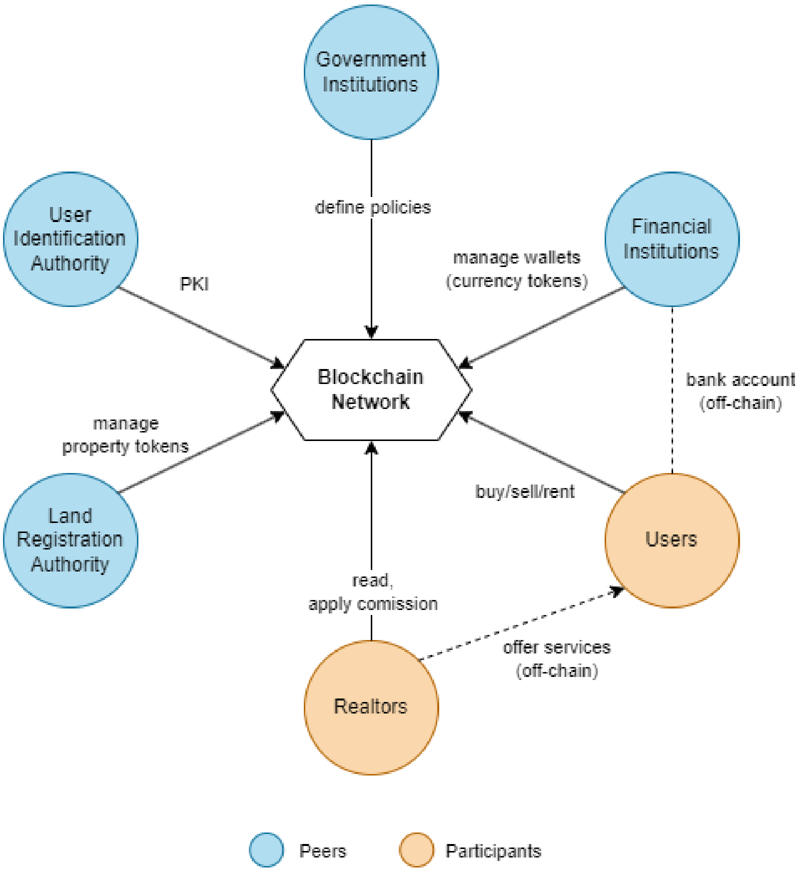

Figure 4.1: Domain Interaction Diagram

4.1 Roles and Stakeholders

Firstly, it is vital to define which stakeholders will be considered in the proposed solution, both those responsible for managing and maintaining the system (peers) and those that will use the system as end users (participants). Figure 4.1 presents a diagram illustrating these entities, and how they engage with the system in terms of what operations they perform within the blockchain network:

Users - The typical end users of the system, representing the average citizens. They might own properties and wish to sell or list them for rent, or they may be seeking to buy or rent properties.

Realtors - Institutes or individuals that aid the users in the process of buying or selling a property, with the goal of facilitating the transaction process. They provide expert guidance on market trends, property valuation, and legal requirements.

Land Registration Authority - The entity responsible for validating the property records, guaranteeing that they comply with the actual physical properties and location of the land. Within the blockchain network, it is responsible for minting and managing the property tokens.

Government Institution - The government body that enforces the country's policies and regulations, ensuring that the system adheres to legal standards.

Financial Institutions - Financial institutions such as banks hold the actual funds of the users and are responsible for relating these funds to the users' accounts on the blockchain network, guaranteeing that the transactions made on-chain are mirrored in the real world.

User Identification Authority - The entity responsible for providing and managing the PKI, by issuing the certificates and linking them to the users' real-world citizen identities.

4.2 System Functionalities & Scope

In this section we define the range of functionalities the proposed solution is predicted to implement, desirably. For the time being, the initial requisites are as follows:

Fractional Ownership - We must assume that a property may belong to multiple entities at the same time, being divided into either dependent or autonomous fractions. Dependent fractions are percentual, meaning that a single property like a household could, for instance, be owned 30% by an entity and 70% by another. Autonomous fractions refer to independent properties that compose a property cluster - an apartment is an autonomous fraction of a building. An autonomous fraction can be further divided into dependent fractions.

Land Conveyance - The main focus of the solution is to support land conveyance. This refers to the process of transferring ownership of a property from one user to another. Due to fractional ownership, we must also consider the possibility of buying and selling individual fractions, instead of the whole property.

Bidding - The sale process of a property must implement a bid-like procedure. When a user lists a property or fraction for sale, it sets the desired selling price but other users are allowed to bid for any price they intend. It is the user who listed the property that must decide if a bid is accepted or not.

Commission Deals - Associated with the sale of a property, there may be a commission taxed by a real estate agent, if one was hired to facilitate the deal process. This tax is usually a percentage of the sale value.

Renting - We also plan to develop a renting system for the properties, featuring rent contracts. In an ideal scenario, we would like to support fully automated recurring payments, meaning the value of the rent would be automatically transferred from the tenant to the landlord(s) every month. There's also the assumption that a rent contract may be prematurely terminated, in which case fees may apply to the party requesting termination. It must be possible to define (at least some of) these policies.

4.3 System Metamodel

Appendix A includes a UML Class Diagram that serves as a metamodel for the proposed solution's architecture. This diagram provides a high-level overview of the system's architecture, primarily focusing on the data that the system will store, how this data should be organized into different entities, and the functions associated with these entities. The relations between these entities illustrate how they are interconnected and associated, which is essential for understanding the overall structure and functionality of the system.

As some might notice, not all of the previously discussed stakeholders are represented as entities in this metamodel. That is the case for the land registry and government bodies, for instance. This is because they do not function as data within the system. Instead, they are external entities that manage or interact with the system's data represented in the diagram. Other stakeholders, like users and realtors, are depicted in the metamodel because they are represented by data structures in the system, such as accounts or addresses.

Additionally, Object Constraint Language (OCL) [32] restrictions were defined to specify the system's behavior for each of the stated functions. OCL is a logic language commonly used to write detailed specifications and constraints for UML models. It allows for the precise definition of rules that the system must adhere to, ensuring that the system's operations are consistent with the intended design and requirements. Due to space limitations of the current deliverable, these OCL restrictions are not present on the Appendix A. However, for those interested, they are available for consultation through [3].

It is important to emphasize that this metamodel does not directly reflect the smart contract architecture of the final solution. Rather, it should be viewed as a guideline that provides information on how the system should be structured and operate. The actual implementation, especially in the context of smart contracts, might have specific nuances and complexities that are adapted to the practicalities of the technology. However, it would be fair to say that, independently from the implementation details, the final solution should comply with the metamodel. Further details regarding the metamodel and the OCL restrictions will be discussed in the final deliverable.

4.4 Design Choices

4.4.1 Network Type

In this section, we explain why we firmly believe that a permissioned consortium blockchain network is preferable for the context of the project, compared to public ones. The first reason is that land registry is by nature a sector that must be regulated by a country's government. Additionally, it involves a multitude of entities that play indispensable roles in the process, each controlling a significant part of it. This complexity and the need for regulation make a consortium blockchain particularly suitable, as it allows for shared control and governance by multiple organizations. Furthermore, many of the advantages offered by public blockchains are not only unnecessary but also undesirable in this context:

1. **Anonymity** - Public blockchains grant anonymity for all network participants. However, in the transaction process of a property, both parties must be unambiguously defined and identified. [7, 22]

2. **Lack of Confidentiality** - Certain data and documents regarding property information or even transactions shall be kept secret from certain entities and the overall public.

3. **Need for Network Administrators** - There may be needed mechanisms for error correction and ownership recovery in case incorrect or fraudulent data is discovered, possibly in the form of multi-signature protocols [22]. Additionally, permissioned chains allow members to come to an agreement and alter previous blocks [16].

4. **Reliance on Public Infrastructure** - Utilizing public infrastructure to control critical national assets, like a country's land registry, poses significant risks and is generally not advisable;

5. **Security Concerns** - Although highly unlikely, there's a possibility of 51% attacks or future threats from quantum computing;

6. **Dependency on Network Traffic** - Transactions in public blockchains are often affected by network congestion, which not only increases the time it takes to confirm them but also leads to higher transaction fees;

7. **Dependency on Native Cryptocurrency** - Public blockchains rely on their own native cryptocurrency for conducting transactions. This dependency would introduce volatility and transaction fees, thus making a part of the transaction value leave the country. It is preferable to use the country's currency for transactions, given the sector's direct linkage to the national economy.

8. **Storage Limitations** - Public blockchains are particularly not suitable for environments that require storing large amounts of data, as their vast node number comes with bandwidth limitations and high transaction costs.

Finally, permissioned blockchains would also provide flexibility in making transactions comply with country-specific legal and tax requirements [21] while providing faster and more efficient transactions with reduced latency.

4.4.2 Development Framework

Following what was previously discussed in section 2.7, we decided to go with Hyperledger Fabric as the blockchain development framework for this work. By looking at Table 2.3, it is obvious why Fabric is among the top contenders for the best framework. But the main reason why we picked it over other contenders lies in that it is highly versatile and general-purpose. Realistically speaking, in a domain like real estate and land registry, it would actually be preferable to pick a more specialized framework for the final solution. R3 Corda, for instance, is specifically designed for financial transactions and has a strong focus on facilitating the legal processes that underpin the financial industry, which is quite relevant to real estate transactions. However, it is also unconventional in the sense that CorDapps do not adhere to a smart contract architecture. The developers themselves have stated that "Corda is both a blockchain and not a blockchain" [35]. Thus, choosing Corda would imply building a Corda-centric solution and architecture. Since this work aims to develop a Proof-of-Concept, the adaptability and applicability of the developed solution becomes a crucial aspect. We aim to provide an architecture that may be used and followed even when using other technologies. Hyperledger Fabric is a generic yet powerful framework capable of utilizing Smart Contracts and even implementing them using Solidity through Hyperledger Burrow.

That said, Fabric is not flawless in every aspect. As shown in section 2.7, Fabric does not inherently support time-based events, which is an important feature if we want to implement fully automated recurring or monthly rent payments in the solution. There are ways to work around this: we could, for instance, resort to a trusted oracle who would emit an event on the network every month that would trigger the rent payments for every rent contract.

4.4.3 Complementary Technologies

Besides the necessary technologies for development in Hyperledger Fabric, such as Docker and Hyperledger Explorer, we predict that necessities may arise related to identity verification, particularly in the implementation of the certificate authorities, and the overall PKI. Additionally, land registries shall contain deeds, names, maps, plans, etc. [22]. This naturally requires the system to store large amounts of data which could be a problem as blockchains' append-only nature may cause the data to grow indefinitely. To address this, there may be a need to recur to a technology like IPFS to store mutable data off-chain. Finally, if we end up developing a client application for demonstration purposes (although this is not a priority), we will utilize additional development frameworks that will be considered based on their ability to integrate with the underlying blockchain technology.

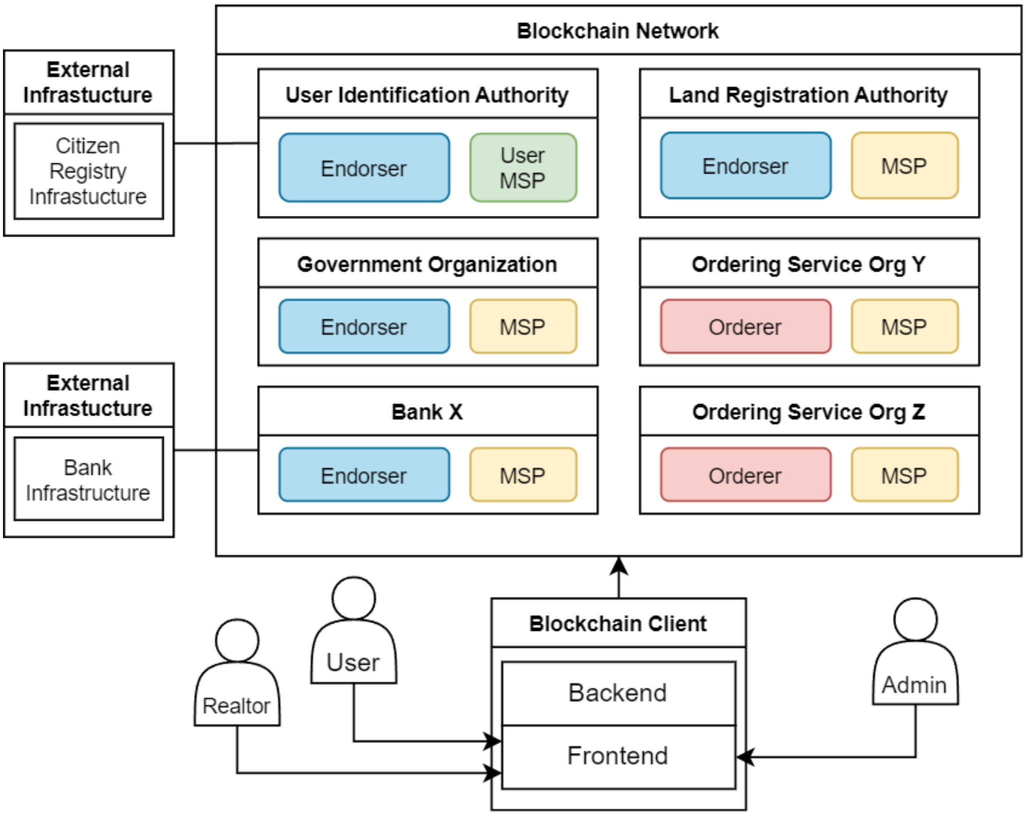

Figure 4.2: Network Overview Diagram

4.4.4 Network Overview

Figure 4.2 shows an early preview of how the network could be structured on Hyperledger Fabric. The presented diagram represents only an abstraction and does not intend to strictly mirror the topology of the final solution. IPFS integration was not considered in this phase, and the diagram does not provide information on the channel configuration or the node number inside each organization.

The peer entities specified in section 4.1 are the endorser organizations, as these are the ones participating actively in the network by approving and signing transactions. The Ordering Service is administered by a different set of authorities, as the ordering peers shouldn't be part of the same organization as the endorsing peers. They are the ones responsible for establishing consensus, but they are essentially agnostic to the content of transactions. They do not need to know anything about the business logic, the participants involved, or the assets being transferred. These authorities could be other government bodies, justice-related institutions such as the courts, or other independent organizations. Furthermore, each organization participating in the network has its own MSP, meaning they are responsible for registering and enrolling users and peers inside their own domain. It is the User Identification Authority, however, who manages the identity verification and authentication for the system's end users, the citizens.

5 Evaluation

We plan to evaluate the developed solution regarding its correctness and performance:

For the performance evaluation, the system will be subjected to multiple tests with varying numbers of peers and client requests. During this process, we will measure and monitor key performance indicators including latency - the time taken for transactions to be confirmed - and throughput - the number of transactions processed per time unit. These metrics are relevant in understanding how the system performs under different conditions and provide insights regarding its efficiency and scalability. Hyperledger Caliper is the blockchain benchmarking tool that we will use for this purpose.

As for the system's correctness, the evaluation will focus on testing the functionality of individual smart contract functions. This will be achieved through the implementation of unit and integration tests, ensuring that each function performs as expected and that they interact seamlessly with the other components of the system. Additionally, the outcomes of chaincode execution will be directly compared to the behavior specified by the provided metamodel, to guarantee that the system complies with the initial specification and rules.

6

Work Plan

Along the course of this project, we plan to organize the work into the following main tasks:

1. **Network Configuration** - The design and configuration of the network topology, involving the characterization of the different node types and roles for each organization, channel architecture, and MSP configuration for a demonstrative PKI.

2. **Chaincode Implementation** - The design and implementation of the smart contracts that encapsulate the business logic, which is the main focus of this work.

3. **Experimental Evaluation** - Extensive testing and evaluation following the methods described in chapter 5.

4. **Demonstrative Client Implementation** (Optional) - The development of a client application that interacts with the proposed system is not a core requirement of the project. However, if the previous activities proceed as planned and we have sufficient time to implement the client, it will be developed to help demonstrate the system's capabilities.

5. **Dissertation Writing** - The writing of the dissertation will take place from the very beginning until the end of the project timeline, following a recurring approach.

Figure 6.1 summarizes the predicted schedule of the described tasks.

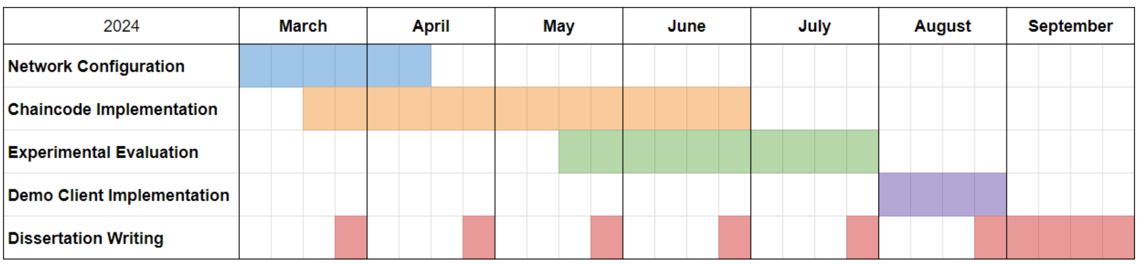

Figure 6.1: Work Plan Schedule

Bibliography

[1] K. M. Alam et al. "A Blockchain-based Land Title Management System for Bangladesh". In: *Journal of King Saud University - Computer and Information Sciences* (2022-06). ISSN: 22131248. DOI: 10.1016/j.jksuci.2020.10.011 (cit. on p. 19).

[2] T. Ali et al. "A transparent and trusted property registration system on permissioned blockchain". In: *International Conference on Advances in the Emerging Computing Technologies, AECT 2019*. Institute of Electrical and Electronics Engineers Inc., 2020-02. ISBN: 9781728144528. DOI: 10.1109/AECT47998.2020.9194222 (cit. on p. 18).

[3] R. Arede. *Blockopoly Repository*. URL: https://github.com/rmarede/Blockopoly (cit. on pp. 28, 38).

[4] ATLANT Platform. "ATLANT Real Estate Platform". URL: https://medium.com/@atlantio/atlant-real-estate-platform-c2b4ef85079d (cit. on p. 24).

[5] A. Averin, P. Rukhlov, and E. Musaev. "Review of Existing Solutions in the Field of Real Estate and Cadastral Accounting Based on Blockchain Technology". In: *Proceedings of the 2021 IEEE International Conference "Quality Management, Transport and Information Security, Information Technologies"*. Institute of Electrical and Electronics Engineers Inc., 2021. ISBN: 9781665433020. DOI: 10.1109/ITQMIS53292.2021.9642802 (cit. on p. 22).

[6] J. Benet. *IPFS - Content Addressed, Versioned, P2P File System*. Tech. rep. (cit. on p. 10).

[7] R. Bennett et al. "Hybrid approaches for smart contracts in land administration: Lessons from three blockchain proofs-of-concept". In: *Land* (2021-02). ISSN: 2073445X. DOI: 10.3390/land10020220 (cit. on pp. 20, 21, 29).

[8] R. M. Bennett, M. Pickering, and J. Sargent. "Transformations, transitions, or tall tales? A global review of the uptake and impact of NoSQL, blockchain, and big data analytics on the land administration sector". In: *Land Use Policy* (2019-04). ISSN: 02648377. DOI: 10.1016/j.landusepol.2019.02.016 (cit. on p. 25).

[9] Binaryx. *Binaryx Website*. URL: https://www.binaryx.com/ (cit. on pp. 23, 24).

[10] R. G. Brown. “The Corda Platform: An Introduction”. 2018 (cit. on p. 11).

[11] A. Castellanos. *Digitalization of Land Records: From Paper to Blockchain*. Tech. rep. 2018 (cit. on p. 22).

[12] J. Chen and S. Micali. “Algorand”. 2016-07. URL: http://arxiv.org/abs/1607.01341 (cit. on p. 12).

[13] Consensys. “Quorum Whitepaper”. 2018. URL: https://github.com/ethereum/wiki/wiki/White-Paper (cit. on p. 11).

[14] Deloitte. *Are token assets the securities of tomorrow?* Tech. rep. 2019 (cit. on p. 10).

[15] Deloitte. *Blockchain in commercial real estate*. Tech. rep. 2017 (cit. on pp. 1, 5).

[16] O. Dib et al. “Consortium Blockchains: Overview, Applications and Challenges”. In: *International Journal on Advances in Telecommunications* 2 (2018) (cit. on pp. 7, 29).

[17] e-estonia. *Estonian blockchain technology FAQ*. Tech. rep. (cit. on p. 22).

[18] e-estonia. *KSI blockchain in Estonia*. Tech. rep. (cit. on p. 22).

[19] European Commission. *Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets (MiCA)*. 2023. URL: http://data.europa.eu/eli/reg/2023/1114/oj (cit. on p. 10).

[20] P. Freni, E. Ferro, and R. Moncada. “Tokenomics and blockchain tokens: A design-oriented morphological framework”. In: *Blockchain: Research and Applications* (2022-03). ISSN: 26669536. DOI: 10.1016/j.bcra.2022.100069 (cit. on p. 9).

[21] R. M. Garcia-Teruel. “Legal challenges and opportunities of blockchain technology in the real estate sector”. In: *Journal of Property, Planning and Environmental Law* (2020-07). ISSN: 25149407. DOI: 10.1108/JPPEL-07-2019-0039 (cit. on pp. 1, 4, 17, 21, 29).

[22] M. Graglia and C. Mellon. *Blockchain and Property in 2018*. Tech. rep. 2018. URL: http://direct.mit.edu/itgg/article-pdf/12/1-2/90/705267/inov_a_00270.pdf (cit. on pp. 29, 30).

[23] G. Greenspan. “MultiChain Private Blockchain” (cit. on p. 11).

[24] A. Gupta et al. “Tokenization of real estate using blockchain technology”. In: *Applied Cryptography and Network Security Workshops*. Vol. 12418 LNCS. Springer Science and Business Media Deutschland GmbH, 2020, pp. -9. ISBN: 9783030616373. DOI: 10.1007/978-3-030-61638-0{_}5 (cit. on pp. 1, 17, 18, 23, 24).

[25] Hyperledger Foundation. *An Introduction to Hyperledger*. Tech. rep. 2018 (cit. on p. 12).

[26] Hyperledger Foundation. *Hyperledger Fabric Documentation*. URL: https://hyperledger-fabric.readthedocs.io/ (cit. on pp. 13, 14).

[27] S. Joshi and A. Choudhury. “Tokenization of Real estate Assets Using Blockchain”. In: *International Journal of Intelligent Information Technologies* (2022). ISSN: 15483665. DOI: 10.4018/IJIIT.309588 (cit. on pp. 17, 18).

[28] I. Karamitsos, M. Papadaki, and N. B. A. Barghuthi. “Design of the Blockchain Smart Contract: A Use Case for Real Estate”. In: *Journal of Information Security* (2018). ISSN: 2153-1234. DOI: 10.4236/jis.2018.93013 (cit. on p. 17).

[29] Lantmäteriet et al. *The Land Registry in the Blockchain - Testbed*. Tech. rep. 2017 (cit. on p. 20).

[30] LaProp. *Tokenized Real Estate*. Tech. rep. 2022 (cit. on p. 24).

[31] S. Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*. Tech. rep. 2008. URL: www.bitcoin.org (cit. on p. 5).

[32] Object Management Group. *Object Constraint Language v2.4*. 2014. URL: http://www.omg.org/spec/OCL/2.4 (cit. on p. 28).

[33] Propy. *Propy Website*. URL: https://propy.com/ (cit. on p. 23).

[34] Propy. “Propy Whitepaper 2.0”. 2021 (cit. on p. 23).

[35] R3. *Blockchain 101*. URL: https://r3.com/blockchain-101/ (cit. on p. 30).

[36] RealT. “Legally Compliant Ownership of Tokenized Real Estate” (cit. on pp. 18, 23, 24).

[37] Rentberry. “Rentberry Whitepaper”. 2018 (cit. on pp. 17, 24).

[38] REX Protocol. *REX Protocol Public Docs*. URL: https://rex-protocol.gitbook.io/rex-protocol-public-docs/ (cit. on p. 24).

[39] A. Saari, J. Vimpari, and S. Junnila. “Blockchain in real estate: Recent developments and empirical applications”. In: *Land Use Policy* (2022-10). ISSN: 02648377. DOI: 10.1016/j.landusepol.2022.106334 (cit. on p. 18).

[40] S. Sen, S. Mukhopadhyay, and S. Karforma. “A Blockchain based Framework for Property Registration System in E-Governance”. In: *International Journal of Information Engineering and Electronic Business* (2021-08). ISSN: 20749023. DOI: 10.5815/ijieeb.2021.04.03 (cit. on p. 19).

[41] L. Shin. “Republic Of Georgia To Pilot Land Titling On Blockchain, BitFury”. In: *Forbes* (2016). URL: https://www.forbes.com/sites/laurashin/2016/04/21/republic-of-georgia-to-pilot-land-titling-on-blockchain-with-economist-hernando-de-soto-bitfury/?sh=27a76a2f44da (cit. on p. 21).

[42] L. Shin. “The First Government To Secure Land Titles On The Bitcoin Blockchain Expands Project”. In: *Forbes* (2017). URL: https://www.forbes.com/sites/laurashin/2017/02/07/the-first-government-to-secure-land-titles-on-the-bitcoin-blockchain-expands-project/?sh=7c4e1894dcdc (cit. on p. 21).

[43] M. Shuaib et al. "Blockchain-based framework for secure and reliable land registry system". In: *Telkomnika (Telecommunication Computing Electronics and Control)* (2020-10). ISSN: 23029293. DOI: 10.12928/TELKOMNIKA.v18i5.15787 (cit. on p. 4).

[44] M. Shuaib et al. "Current Status, Requirements, and Challenges of Blockchain Application in Land Registry". In: *International Journal of Information Retrieval Research* (2022-08). ISSN: 2155-6377. DOI: 10.4018/ijirr.299934 (cit. on pp. 1, 4, 5, 21).

[45] M. Shuaib et al. *Identity Model for Blockchain-Based Land Registry System: A Comparison*. 2022. DOI: 10.1155/2022/5670714 (cit. on p. 1).

[46] W. Stallings. *Network Security Essentials: Applications and Standards*. Prentice Hall, 2011, p. 417. ISBN: 0136108059 (cit. on p. 8).

[47] Statista. *Real Estate Worldwide*. Tech. rep. URL: https://www.statista.com/outlook/fmo/real-estate/worldwide (cit. on p. 1).

[48] N. Szabo. *Smart Contracts*. 1994. URL: https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html (cit. on p. 9).

[49] Tokeny. *T-REX Protocol (Token for Regulated EXchanges) Whitepaper*. Tech. rep. 2023. URL: https://github.com/TokenySolutions (cit. on p. 10).

[50] USAID. *Honduras | LandLinks*. Tech. rep. 2011. URL: https://www.land-links.org/country-profile/honduras/ (cit. on p. 22).

[51] World Bank. *Doing Business Report - Registering Property*. Tech. rep. 2019. URL: https://archive.doingbusiness.org/en/data/exploretopics/registering-property (cit. on p. 21).

[52] H. P. Wouda and R. Opdenakker. "Blockchain technology in commercial real estate transactions". In: *Journal of Property Investment and Finance* (2019-08). ISSN: 1463578X. DOI: 10.1108/JPIF-06-2019-0085 (cit. on p. 1).

[53] D. Yaga et al. "Blockchain Technology Overview". In: (2019-06). DOI: 10.6028/NIST.IR.8202 (cit. on pp. 7, 8).

[54] Z. Zheng et al. "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends". In: *Proceedings - 2017 IEEE 6th International Congress on Big Data, BigData Congress 2017*. Institute of Electrical and Electronics Engineers Inc., 2017-09, pp. 557–564. ISBN: 9781538619964. DOI: 10.1109/BigDataCongress.2017.85 (cit. on p. 6).

A

System Metamodel

The high-level metamodel of the system architecture mentioned in section 4.3. The OCL restrictions defined for each of the specified functions are available in the Blockopoly Github repository [3].