الجمهورية الجزائرية الديمقراطية الشعبية

The People's Democratic Republic of Algeria

وزارة التعليم العالي والبحث العلمي

Ministry of Higher Education and Scientific Research

جامعة محمد بوضياف بالمسيلة

University Mohamed Boudiaf of M'sila

كلية الرياضيات والإعلام الآلي

Faculty of Mathematics and Informatics

قسم الإعلام الآلي

Department of Computer Science

Domain: Computer Science

Thesis Presented to Fulfill the Partial Requirement

for **Master's Degree** in Computer Science

Specialty: Artificial Intelligence

Entitled

Blockchain-Based Tokenized Object Sales: Application in the Automotive Industry.

Prepared By: Mekki Fayssal, Touami Djelloul

Supervised By: Adel Moussaoui

Jury Members

Makhlouf Benazi	President
Adel Moussaoui	Supervisor
Abdessattar Ghemougui	Examiner

Academic Year 2024/2025

Dedication

To my mother, whose quiet strength and boundless kindness carried me forward,
and to my father, whose wisdom and steady support lit the path before me—
thank you for being my foundation.

To my siblings, who shared the weight of this journey with laughter, encouragement, and love,
your presence made the hard days easier and the good days even better.

And to all the mentors and friends who shaped my academic journey,
this thesis is not mine alone—it is a reflection of your impact and shared perseverance.

Mekki Fayssal

To my parents, Thank you for your love, your prayers, and your countless supports.
You have been my greatest support, and I owe this journey to you.

To my brothers and sisters,Thank you for being there through the ups and downs.
Your encouragement and laughter gave me strength when I needed it most.

To my teachers, friends, and everyone who helped me along the way This thesis is a result of your kindness, guidance, and belief in me.

Touami Djelloul

Acknowledgement

First and foremost, we are deeply grateful to **Allah**, whose guidance, strength, and patience have sustained us throughout this journey and made this achievement possible.

We extend our sincere thanks to Mr.Adel Moussaoui, our respected supervisor, for his valuable guidance and ongoing support. His encouragement and insightful comments have greatly contributed to the progress and quality of our project.

Our heartfelt appreciation also goes to our families, friends, and colleagues. Your constant support, encouragement, and belief in us have been a source of motivation at every step.

Thank you all for being part of this journey.

Abstract:

This project focuses on the tokenization of physical objects, particularly cars, for sale and transfer through blockchain platforms. Tokenization enables each car to be represented by a unique digital token that can be traded or sold securely and transparently on a blockchain network. The project will address how smart contracts can facilitate the sales process, including ownership transfer, payment, and compliance with regulations. The system will also explore reducing fraud, improving trust between buyers and sellers, and speeding up the sales process.

Keywords: Tokenization, Blockchain, Solana, Smart Contracts, Cryptocurrency, vehicles, decentralized works, transfer of ownership, transparency , anti-fraud, Web 3.0, traceability.

الملخص:

يركز هذا المشروع على ترميز (Tokenization)الأصول المادية، وتحديداً السيارات، لغرض البيع ونقل الملكية عبر منصات البلوك تشين (Blockchain).يُمكّن الترميز من تمثيل كل سيارة برمز رقمي فريد يمكن تداوله أو بيعه بشكل آمن وشفاف على شبكة البلوك تشين .سيتناول المشروع كيف يمكن للعقود الذكية (Smart Contracts)تسهيل عملية البيع، بما في ذلك نقل الملكية، والدفع، والامتثال للوائح التنظيمية .كما سيبحث النظام في الحد من الاحتيال، وتعزيز الثقة بين المشترين والبائعين، وتسريع عملية البيع.

الكلمات المفتاحية: الترميز الرقمي، سلسلة الكتل ، Solana، العقود الذكية، العملات الرقمية، المركبات، الأعمال اللامركزية، نقل الملكية، الشفافية، مكافحة الاحتيال، Web 3.0، إمكانية التتبع.

Résumé:

Ce projet se concentre sur la tokénisation (ou titrisation numérique) d'objets physiques, en particulier les voitures, pour leur vente et transfert via des plateformes blockchain. La tokénisation permet que chaque voiture soit représentée par un jeton numérique unique qui peut être échangé ou vendu de manière sécurisée et transparente sur un réseau blockchain. Le projet examinera comment les contrats intelligents (smart contracts) peuvent faciliter le processus de vente, y compris le transfert de propriété, le paiement et la conformité réglementaire. Le système explorera également la réduction de la fraude, l'amélioration de la confiance entre acheteurs et vendeurs, et l'accélération du processus de vente.

Les Mots clés : Tokenisation, Blockchain, Solana, Smart Contracts, Cryptomonnaie, véhicules, œuvres décentralisées, transfert de propriété, transparence, anti-fraude, Web 3.0, traçabilité.

Contents

List of Figures

Introduction

Since its inception, the Internet has witnessed rapid evolution. It began as a mere tool for information transfer, then progressed to a more interactive phase with the advent of Web 2.0, which enabled users to exchange content and participate in digital platforms. As development continued, the concept of Web 3.0 emerged, no longer viewed merely as a means of communication and interaction but as a platform for transferring value and digital ownership securely and reliably, without the need for intermediaries.

Web 3.0 relies on a set of advanced technologies that paved the way for this transformation. Among the most prominent of these technologies is blockchain, which provides a decentralized and secure environment for storing data and conducting transactions. In this research, we will explore the role of these technologies in developing decentralized applications, with a focus on implementing a specific application in the automotive sector based on digital coding and blockchain.

Chapter One

Web 3.0 : Blockchain and Digital Assets

1.1. Introduction

In this Chapter , we will discover the main technology which help the web 3.0 to get high push to which are the blockchain and tokenization

1.1. Blockchain

1.1.1. Overview of Blockchain

Blockchain is one of the most important technologies used in decentralized applications and cryptocurrencies. However, its origins were unrelated to the latter. The initial idea of blockchain first appeared in 1991 when cryptographer David Chaum proposed the concept of a decentralized system for securely storing data in his scientific paper titled: "Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups." In 1992, this idea was further refined by Stuart Haber, W. Scott Stornetta, and Dave Bayer, who introduced the concept of the Merkle Tree, enhancing the system's efficiency and ability to secure data in a tamper-proof manner.[1] By 2008, a person or group under the pseudonym Satoshi Nakamoto introduced a digital currency called Bitcoin, which relied on this technology.[1]

Blockchain is a decentralized digital ledger that operates across a network of computers known as **nodes**. This technology is characterized by its immutability and tamper-proof nature, relying on cryptographic techniques to ensure data integrity. New data can only be added to the chain, and previously stored data cannot be modified unless a majority of nodes agree. This makes the system trustworthy and secure against manipulation. One of its most famous uses is recording cryptocurrency transactions[2].

Blockchain technology relies on the principle of storing data in sequential blocks linked together using advanced cryptographic techniques. Information and transactions are grouped into a block of a specific size. Once the block is complete, a unique digital fingerprint is generated using a hash function. This fingerprint, known as the block header, represents the block's content in an irreversible manner. Any minor change in the block's content results in a drastic change in the hash value. When the next block is created, it includes information from the previous block, including its hash value. A new block header is then generated for the new block using the same function. This creates an interconnected chain of blocks (blockchain), where each block is linked to its predecessor. This linkage makes it impossible to modify any previous block without affecting all subsequent blocks, as any alteration would change the hash of the modified block and all following blocks. Thus, any attempt to tamper with the data would be immediately apparent, ensuring transparency and security.

1.1.2. Types of Blockchain:

Blockchain networks are generally classified into two main types: permissionless and permissioned.

- In **permissionless blockchain**, anyone can modify and add blocks without prior authorization, reinforcing the principle of decentralization and openness to all entities.
- In **permissioned blockchain**, only a specific group of individuals is allowed to modify and manage blocks.

Bitcoin is an example of a permissionless blockchain, though it relies on special mechanisms and protocols called consensus mechanisms to regulate modifications, preventing unwanted entities from accessing the network.[3]

1.1.3. Consensus Mechanisms

Consensus mechanisms are one of the foundational pillars of blockchain technology. They are defined as the means by which all **nodes** in a distributed network reach a common agreement on the validity of data added to the blockchain. This system enables the network to operate synchronously and reliably, even in the absence of a central authority controlling the processes.[4]

Consensus mechanisms are fundamental to blockchain technology, playing a pivotal role in enhancing security, integrity, and network stability. These mechanisms penalize fraudulent or malicious behavior by imposing penalties on nodes attempting to manipulate data, ensuring system integrity and protecting it from internal or external attacks. Additionally, consensus mechanisms not only penalize untrustworthy behavior but also incentivize honesty by rewarding nodes that follow the rules. This dual system of penalties and rewards strengthens network stability and builds user trust. One of the key challenges addressed by consensus mechanisms is the Byzantine Fault Tolerance (BFT) problem. This issue involves achieving consensus among a group of nodes in distributed systems when some are untrustworthy or act maliciously. In blockchain, nodes represent "soldiers," while distributed data represents "orders." The solution lies in robust consensus mechanisms like Proof of Work (PoW) or Proof of Stake (PoS), which ensure system continuity even in the presence of faulty or malicious nodes.[5] Furthermore, consensus mechanisms enhance decentralization, a defining feature of blockchain technology. Through these mechanisms, anyone can participate in the network without needing a central intermediary, reducing operational costs and mitigating risks associated with third-party reliance.

1.1.3.1. Proof of Work (PoW):

Proof of Work (PoW) is one of the most common consensus mechanisms in blockchain technology. It was initially developed in 1993 by researchers Cynthia Dwork and Moni Naor to combat spam and Denial-of-Service (DoS) attacks. The theoretical idea was to force senders to perform complex computational tasks, making cyberattacks costly and impractical.[6]

Later, in 1997, researcher Adam Back developed a practical model for this idea called Hashcash, which imposed computational tasks on senders before transmitting messages, with easy verification of solutions. One of Hashcash's key features was its adjustable computational difficulty.[7]

In 2008, Satoshi Nakamoto implemented PoW in the Bitcoin network, revolutionizing the world of cryptocurrencies. The primary goal of this mechanism was to prevent double-spending and forgery by verifying transaction validity, creating scarcity by capping the

number of mineable Bitcoins, and securing the network by making blockchain modifications computationally and energetically expensive.

In the Bitcoin network, miners compete to solve complex mathematical puzzles related to finding a nonce (a random number) so that the resulting block hash meets a specified difficulty condition, such as starting with a certain number of zeros. This condition is adjusted every 2016 blocks (approximately every two weeks) to maintain a stable block mining rate of 10 minutes per block.[8]

PoW plays a fundamental role in network security through several mechanisms, including:

- The high cost of any attack requiring control over more than 50% of the network's computational power (51% attack).
- Multiple verifications of block and transaction validity.
- The ease of verifying solutions compared to the difficulty of finding them.

While a theoretical breach is possible if most computational power is controlled, the high economic and technical costs make this scenario impractical, especially for large networks like Bitcoin.[8]

1.1.3.2. Proof of Stake (PoS)

Proof of Stake (PoS) is a class of consensus algorithms designed to achieve distributed agreement in blockchain networks, presenting a alternative to the computationally intensive Proof of Work (PoW) paradigm. A principal driver for the exploration and adoption of PoS has been the considerable energy consumption associated with PoW-based systems. For instance, the Bitcoin network, which utilizes PoW, has an estimated annual energy consumption of approximately 91 Terawatt-hours (TWh) (Digiconomist, n.d.). This level of energy usage is substantial, reportedly exceeding the annual consumption of sovereign nations such as Finland or Egypt.[9] Such high energy demands are an inherent consequence of PoW's reliance on competitive, resource-intensive computational tasks to validate transactions and secure the network. Consequently, PoS has emerged as a compelling alternative, offering the potential for comparable security and decentralization with significantly reduced energy expenditure and a more favorable environmental profile.

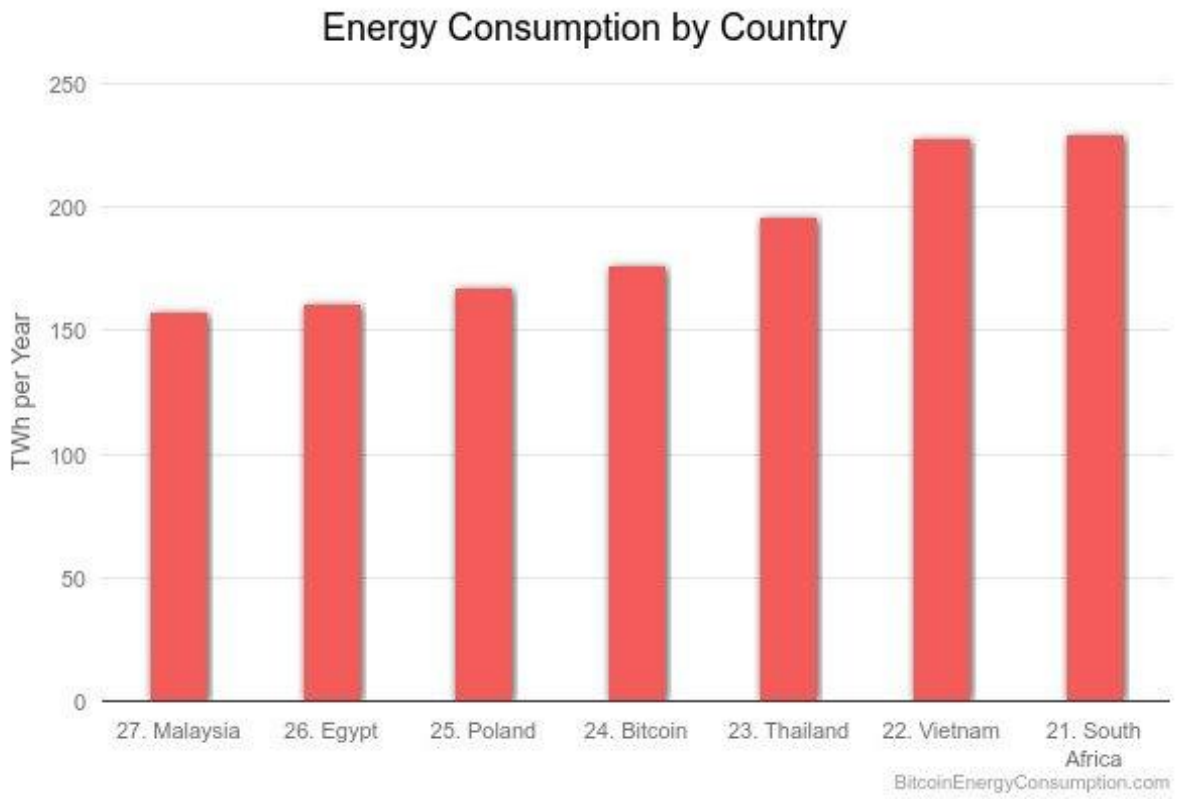

Figure 1 Energy Consumption by Country[9]

The fundamental objective of any blockchain consensus mechanism is to enable the secure and auditable addition of new blocks of transactions to the distributed ledger, thereby establishing a consistent and agreed-upon "truth" across all network participants. A critical aspect of achieving this is to impose a cost or disincentive against malicious behavior, such as attempts to fraudulently alter the ledger or introduce invalid blocks. In PoW, this cost is primarily manifested through the expenditure of computational resources and electrical power. In contrast, PoS mechanisms shift this cost paradigm from computational work to economic stake, wherein participants (validators) commit a portion of their cryptocurrency holdings as collateral to participate in the consensus process.

In a PoS system, the right to validate transactions and propose new blocks is typically assigned to network participants, termed "validators" (or "stakers," "minters" in some contexts), based on the quantity of the network's native cryptocurrency they possess and are willing to "stake" or lock up as collateral. This contrasts markedly with PoW, where the probability of successfully mining a block is directly proportional to a miner's share of the total network computational power (hash rate). Validator selection in PoS can be implemented through various methods, but it generally aims to be pseudo-random, with the probability of selection often weighted by the size of the stake. The larger the stake a participant commits, the higher their likelihood of being chosen to propose a new block or attest to its validity. Once a validator proposes a block, other validators (or a committee thereof) will attest to its validity. If a sufficient number of attestations are gathered, the block is considered confirmed and appended to the blockchain. Validators are typically rewarded with transaction fees

and/or newly minted tokens for their honest participation. Conversely, dishonest behavior, such as attempting to double-spend or validating fraudulent transactions, can result in penalties, most notably "slashing," where a portion or all of the validator's staked assets are forfeited.[10]

Ethereum's transition to PoS ("The Merge") provides a prominent example of a sophisticated PoS implementation. In this model:

- **Eligibility:** To become a validator, a user must deposit 32 ETH into a designated smart contract and operate three distinct software clients: an execution client (to process transactions), a consensus client (to manage the PoS protocol), and a validator client (to manage the validator's keys and duties).
- **Network Timing:** The network operates in discrete time units called "slots" (12 seconds each), which are grouped into "epochs" (32 slots).
- **Block Proposer Selection:** For each slot, a single validator is pseudo-randomly selected from the active validator set to propose a new block. Mechanisms like RANDAO, which aggregate randomness contributions from multiple validators, are employed to ensure unpredictability and fairness in this selection.
- **Attestation Committees:** For each epoch, the active validator set is divided into committees, with validators in each committee assigned to attest to blocks proposed during specific slots within that epoch.
- **Block Creation and Propagation:**

    1. The **execution client** of the chosen block proposer gathers transactions from its local mempool, executes them, and bundles them into an "execution payload."
    2. This payload is passed to the **consensus client**, which incorporates it into a "beacon block" (the PoS block structure).
    3. The beacon block is then propagated across the consensus layer's peer-to-peer (gossip) network.

- **Attestation and Finality:**

    4. Assigned validators receive the proposed block and, using their **validator client**, attest to its validity. These attestations are broadcast to the network.
    5. A block (and by extension, its transactions) is considered "finalized" when it has been linked into the canonical chain by a "supermajority link" between two checkpoints (typically the first block of an epoch). This requires attestations from over two-thirds of the total staked ETH. The earlier checkpoint becomes finalized, while the more recent one becomes "justified," awaiting further attestations in the subsequent epoch to achieve finality.
    6. If the network fails to reach a supermajority agreement for a sufficient period (e.g., four epochs), an "inactivity leak" mechanism can be activated. This progressively reduces the stake of non-participating (offline or non-attesting) validators, ensuring that the chain can eventually regain the supermajority required for finality.

- **Incentives and Disincentives:** Validators receive rewards for proposing blocks and making timely attestations. Conversely, malicious actions or prolonged inactivity can lead to slashing of their staked ETH, providing a strong economic disincentive against detrimental behavior.[10]

The PoS consensus mechanism, in its various iterations, has been adopted by a significant and growing number of blockchain networks. Ethereum's transition is a landmark event, but other prominent platforms have long utilized or have been designed with PoS or its variants. These include, but are not limited to, Cardano (Ouroboros family of PoS protocols), Solana (which employs a hybrid model incorporating Proof of History with PoS), Tezos (Liquid PoS), Tron (Delegated PoS), and Aptos (Kraken, n.d.; specific protocols vary). This widespread adoption underscores its perceived benefits in terms of scalability, energy efficiency, and potentially lower barriers to entry for network participation compared to capital-intensive PoW mining.[11]

1.1.4. Smart Contract

A smart contract is a self-executing script stored on the blockchain. It can execute autonomously without the need for intermediaries and helps translate business logic into clear contract terms. It first appeared in Ethereum and has evolved significantly with newer blockchains. Gartner estimates that by 2022, over 25% of global organizations will use smart contracts. [12]

1.1.5. Supporting Blockchain Technologies

1.1.5.1. Merkle Tree:

Merkle Trees (also known as Binary Hash Trees) are encrypted data structures used to ensure data integrity in blockchain systems. This structure works by generating a shared hash for each pair of leaves, then placing the output in a non-primary branch (Branch). Pairs of branches are then merged and repeatedly hashed until reaching the primary root (Merkle Root), which represents the final hash summarizing all data in the tree. This mechanism is used in blockchain to validate transactions efficiently, allowing nodes to verify transactions without storing all data, enhancing security and computational efficiency.[13]

1.1.5.2. Asymmetric Encryption:

In blockchain, asymmetric encryption ensures transaction security and user identity verification. This encryption uses a key pair:

- **Public Key**: Used to derive user addresses within the network and **verify digital signatures** created by the private key. As it isn’t used for signing, it requires no strict protection.
- **Private Key**: Used to digitally sign transactions, proving ownership of digital assets linked to the address. Due to its sensitivity, this key must remain secret—its loss or leakage may result in loss of asset control.

This mechanism validates transactions without exposing private keys, enhancing blockchain security and reliability.[3]

1.1.5.3. Wallets:

Digital wallets are software designed to securely manage cryptographic addresses. They allow users to store private/public keys and associated addresses, enabling effective digital asset management. These wallets provide user-friendly interfaces for sending/receiving cryptocurrencies and protect private keys from theft or loss. Storage methods vary.[3]

Popular wallets today include **MetaMask**, **Trust Wallet**, and **Phantom**, which support multiple networks/cryptocurrencies and let users manage assets easily and securely.

1.1.6. Blockchain Networks

1.1.6.1. Bitcoin:

Bitcoin is the first and most famous practical application of blockchain technology. It debuted in 2008 when the pseudonymous Satoshi Nakamoto published a whitepaper titled:
"Bitcoin: A Peer-to-Peer Electronic Cash System"
Nakamoto proposed a decentralized system for value transfer without financial intermediaries. On January 12, 2009, the first Bitcoin transaction occurred when Nakamoto sent 10 BTC to cryptographer Hal Finney, making him Bitcoin's first recipient.

Bitcoin is a cryptographic peer-to-peer (P2P) digital currency relying on blockchain for security and trust. Key features:

- **Decentralization**: No government or financial institution controls it.
- **Security & Transparency**: All transactions are recorded on the immutable blockchain.
- **Limited Supply**: Capped at 21 million BTC, preventing inflationary unlimited issuance.

A Bitcoin transaction undergoes several stages:

1. The sender signs the transaction with their private key to prove ownership.
2. The transaction broadcasts to the Bitcoin network and enters the mempool (pending confirmation).
3. Miners validate the transaction to prevent double-spending.
4. Valid transactions are grouped into a new block using a Merkle Tree, and the block's SHA-256 hash is calculated.
5. Mining uses Proof of Work (PoW): Miners solve mathematical puzzles by adjusting a nonce until the hash meets the target difficulty. The first miner to solve it earns

the block reward (currently 6.25 BTC, halving every 210,000 blocks until block 6,929,999).

6. Confirmed blocks join the blockchain, finalizing transactions.

Despite Bitcoin's security and transparency, it lacks smart contract support (preventing DApp development) and handles only ~7 transactions/second, leading to high fees and delays.[14]

1.1.6.2. Ethereum:

Ethereum is a decentralized blockchain with smart contract functionality. Ether is the native cryptocurrency of the platform. Among cryptocurrencies, ether is second only to bitcoin in market capitalization. It is open-source software.Ethereum was conceived in 2013 by programmer Vitalik Buterin. Other founders include Gavin Wood, Charles Hoskinson, Anthony Di Iorio, and Joseph Lubin. In 2014, development work began and was crowdfunded, and the network went live on 30 July 2015. Ethereum allows anyone to deploy decentralized applications onto it, with which users can interact. Decentralized finance (DeFi) applications provide financial instruments that do not directly rely on financial intermediaries like brokerages, exchanges, or banks. This facilitates borrowing against cryptocurrency holdings or lending them out for interest. Ethereum also allows users to create and exchange non-fungible tokens (NFTs), which are tokens that can be tied to unique digital assets, such as images. Additionally, many other cryptocurrencies utilize the ERC-20 token standard on top of the Ethereum blockchain and have utilized the platform for initial coin offerings.

On 15 September 2022, Ethereum transitioned its consensus mechanism from proof-of-work (PoW) to proof-of-stake (PoS) in an update known as "The Merge", which cut the blockchain's energy usage by 99%.

Ethereum was initially described in late 2013 in a White paper by Vitalik Buterin, a programmer and co-founder of Bitcoin Magazine, that described a way to build decentralized applications. Buterin argued to the Bitcoin Core developers that blockchain technology could benefit from other applications besides money and that it needed a more robust language for application development that could lead to attaching real-world assets, such as stocks and property, to the blockchain. In 2013, Buterin briefly worked with eToro CEO Yoni Assia on the Colored Coins project and drafted its white paper outlining additional use cases for blockchain technology. However, after failing to gain agreement on how the project should proceed, he proposed the development of a new platform with a more robust scripting language a Turing-complete programming language that would eventually become Ethereum.

1.1.6.3. Solana:

Launched in 2017 by Anatoly Yakovenko, Solana is a high-performance blockchain designed to improve speed and reduce costs. Its innovation is Proof of History (PoH), which timestamps transactions without constant node communication, enabling parallel transaction processing.[15]

1.1.6.3.1. Solana's Network Design:

Solana uses a dynamic leader system:

- A leader creates the PoH sequence.
- Validators verify the sequence.
- Leaders are chosen via Proof of Stake (PoS), enhancing security/efficiency .[15]

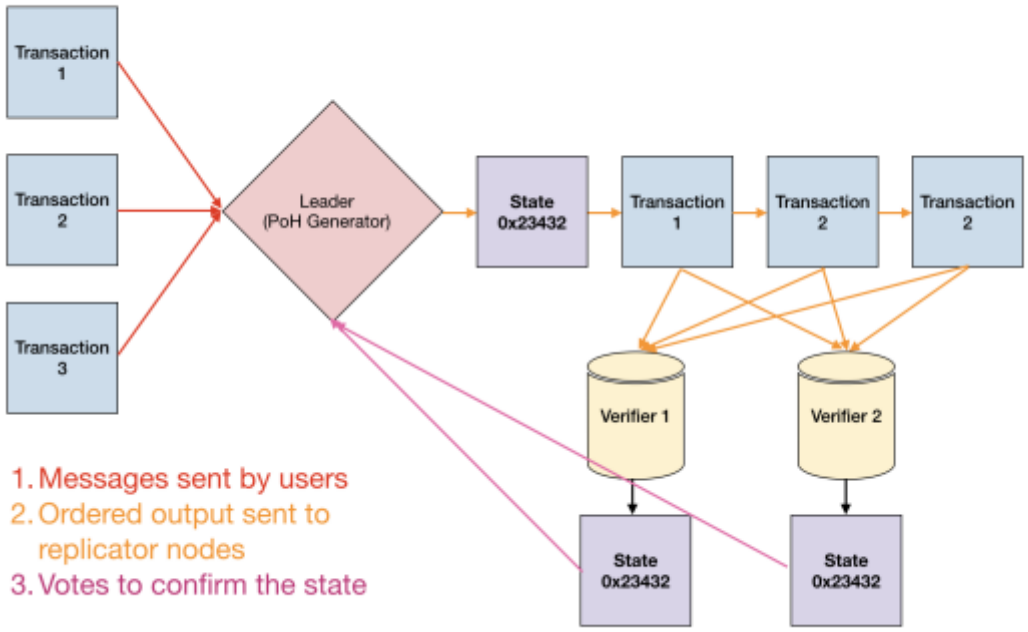

Figure 2:Diagram of how solana work.[15]

1.1.6.3.2. Proof of History (PoH):

Proof of History (PoH) in Solana is an innovative technology used to enhance network performance, though it is not a consensus mechanism—Solana primarily relies on Proof of Stake (PoS) for consensus.

PoH operates as a sequential chain of computations that provides cryptographic verification of the time elapsed between two events. The output of the first operation is used in the second, the second in the third, and so on. Because these operations are sequential and interdependent, they cannot be executed across multiple CPU cores simultaneously—meaning the sequence must be generated on a single core. However, verification can be done efficiently in parallel by splitting the block into multiple segments and validating each segment independently.

By embedding transactions in the hash chain, PoH allows the network to confirm that Transaction X occurred before the subsequent hash. Just as Hash #500 cannot be known without computing all prior hashes, PoH ensures precise chronological ordering. The sequential nature of these functions prevents parallel generation but enables highly efficient

parallel verification—modern computers can divide the chain into 4,000 segments and validate them concurrently.

These properties allow all nodes in the network to determine the exact timing and order of transactions without requiring continuous coordination, significantly boosting reliability. PoH is fundamental to Solana's high-performance architecture, enabling transaction speeds far exceeding traditional blockchains and making it one of the fastest scalable networks available.[15]

1.1.6.3.3. Solana's Features:

Solana is a modern blockchain network that supports smart contracts while delivering high performance and extremely low transaction costs, making it an ideal platform for developing decentralized applications. The network leverages innovative technologies to improve transaction speeds and reduce fees, setting it apart from traditional blockchains.

Transaction Speed

Transaction speed is critically important in blockchain networks for trading and commerce operations.

- **Bitcoin Network:** Processes an average of 7 transactions per second (TPS)[16], with each block confirmation taking approximately 10 minutes. This relatively low efficiency stems from its Proof of Work (PoW) consensus mechanism, which prioritizes security and decentralization over speed.
- **Ethereum Network:** Handles around 15-30 TPS under its Proof of Stake (PoS) system, with expectations for higher throughput as scaling solutions are implemented.
- **Solana Network:** Stands out with its high-performance capability, processing up to 65,000 TPS, making it one of the fastest blockchain networks available today.[17]

Fee Comparison

Transaction fees vary significantly across networks depending on congestion and consensus mechanisms.

- **Bitcoin:** Fees typically range from a few cents to several dollars and can exceed $20 during peak times. These fees are paid to miners, who prioritize transactions with higher fees.
- **Ethereum:** Known for relatively high gas fees, often exceeding $1 per transaction, especially during periods of heavy network congestion.
- **Solana:** Features ultra-low transaction costs, averaging just $0.00025 per transaction, making it highly attractive for applications requiring high-frequency transactions with minimal operational expenses.[18]

Solana's combination of blazing-fast speeds and near-zero fees positions it as a leading choice for scalable decentralized applications.

1.2. Tokenization and Digital Assets

Tokenization and digital assets are important components of Web 3.0 and represent the starting point for digitizing real-world objects.

1.2.1. Digital Assets

Digital assets are anything that is created or stored digitally, can be identified and explored, and have value. This definition includes a wide variety of assets such as images, documents, videos, cryptocurrencies, and tokenized assets.[19]

1.2.2. Asset Tokenization

Asset Tokenization is the process of representing asset ownership as a digital token stored on a blockchain. It acts like a digital certificate of ownership and can represent physical objects, digital assets, fungible tokens, or non-fungible tokens (NFTs). Major companies like Microsoft and Vanguard have already launched projects to tokenize industrial assets and securities.

The tokenization process relies on blockchain networks that support smart contracts. The first step is selecting the asset—this could be commodities, money, securities, or even cars. Next, you choose the token type and standard (we'll explore this further in the next section), as well as define the minting mechanism and any rules governing the token. After that, selecting the appropriate blockchain network is crucial. Verifying the off-chain asset comes next—this means confirming that the asset truly exists in the real world and has a verifiable, reliable value before minting the token. Finally, the token is securely minted and deployed to the blockchain.[20]

1.2.3. Token Standards

Token Standards is the set of rules, protocols, specifications which determine how the token act in the blockchain ecosystem and this have curcial rule in organize the bevior of the tokens and keeping the consistensy in handling with it. And easiness of compitablilty when working with applications and wallets and other platforms. The Standards help to achieve interoperability between deffernt system and easy and secure and smooth use specially in digital assets management.[21]

1.2.3.1. Ethereum Standards:

In Ethereum there's standards for fungible tokens Like ERC 20 and standards for NFT like ERC 721 and ERC 1155 and there is many tokens but the last mentioned is the popluar

https://ethereum.org/en/developers/docs/standards/tokens/

ERC-20 Standards: One of the most important standards in etherum netwoerk and used for creating fungible token and is unhance the development process. And if the token is created with ERC-20 standards, it will work smoothly with other wallets and smart contracts and other applications.[22]

ERC-721 Standards: the official standard for NFT in ethereum and give the cappability for create unique token with unique value even if it issued by the same smart contract make on considration the rarity, age and visuales themes and others.[23]

ERC-1155 Standards: A Standards for multi Token which is give the cappablity of Erc 20 and erc721 and also the capablity for illumted tokens with defferent types and ussually it's contain content like metadata , supply and the traits and indepenadent behavior.[24] [25]

1.2.3.2. Solana Standards

In solana every data is stored in accounts , solana is like a big databases with single table "Accounts" with the same Account type.

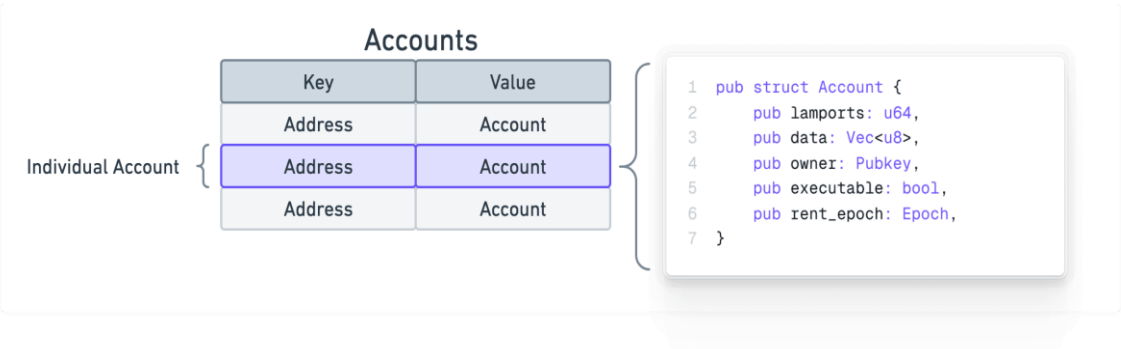

Figure 3 Illustration about accounts in solana

And data field register the program accounts if is porgram or the arbitrary data for an account in not. And the executable field is determine if this is program or data account.
"owner: The program ID (public key) of the program that owns this account. Only the owner program can change the account's data or deduct its lamports balance."[26]

The solana have official standards to create tokens which is spl(solana program library) token. Spl token programs which contain the instractions for interacting with tokens. The mint account which represents specific token and stores metadata about tokens such as the total supply and mint authority.Token Account this is like the wallet which contain token so every person want to own the token it need token account, Associated token account(ATA) is account created using the user address and the token adress to make it easy to find the the token or user.[27]

CHAPTER Two:

The state of the car trade in Algeria

2.1. Overview of the market

Understanding the traditional system helps shed light on the pain points experienced by various stakeholders in the property transfer process, particularly citizens. It also allows us to identify areas that can be improved through the use of blockchain or traditional technologies. The current system faces several challenges, which we will discuss later after outlining the buying and selling **framework in Algeria.**

Given the variety of car sales and purchase scenarios—such as buying a new car versus a used one, or an imported car versus a locally manufactured one—this study will focus on the case of purchasing used locally manufactured cars, as they are the most common and widely traded in the market.

2.2. Traditional Purchase Process Flow

The sale of a used car begins when the seller lists their vehicle through traditional marketing channels, such as local markets, or digital platforms like **Ouedkniss** or **Facebook Marketplace**. After communicating with an interested buyer, the two parties (the seller and the buyer) agree on a price, and the buyer pays the agreed-upon amount.

In the next stage, both parties go to the municipality, accompanied by a sales declaration (such as the one attached in Appendix 1) and the vehicle's registration card, to have it authenticated by the relevant administrative authorities and remove the seller's name from the card. They then proceed to the appropriate tax office to pay the vehicle tax, where the buyer receives a payment receipt and purchases the required fiscal stamp. At this point, the seller's role is complete.

الجمهوريـــة الجزائريـــة الديمقراطيـــة الشعبيـــة

ولايـــة: الرقم:..... التاريخ:.....

دائرة أو الدائرة الإدارية:

بلديـــة:

تصريـــــح بالبيـــــع

(كل تصريح فيه زيادة أو شطب لا يكون صالحا)

أنا السيد (ة): ..... ابن(ة):..... و.....

تاريخ و مكان الميلاد:.....

الجنسية: ..... المهنة: .....

العنوان:.....

أصرح ببيع مركبتي ذات المواصفات التالية:

النوع:..... الصنف:..... الطراز :.....

الرقم التسلسلي في الطراز :..... الهيكل:..... الطاقة: .....

القوة:..... عدد المقاعد: .....جملة الحمولة المرخصة: .....

الحمولة المقيدة: ..... سنة أول استعمال في السير:.....

رقم التسجيل السابق:..... رقم التسجيل الحالي: .....

إلى السيد(ة):

الاسم و اللقب: ..... ابن(ة):..... و.....

تاريخ و مكان الميلاد:.....

الجنسية: .... المهنة:.....

العنوان: .....

كما أشهد بأن هذه المركبة مازالت مطابقة لآخر محضر للقبول صادر من مصلحة المناجم.

حرر ب:..... في:.....

توقيع و بصمة السبابة اليسرى للبائع المصادق عليهما من طرف ضابط الحالة المدنية

ب.ت.و .أو ر.س. رقم:.....

الصادرة في:..... الاسم و اللقب بالحروف اللاتينية:

من طرف: ....

ملاحظة: * يمكن أن يصادق على التوقيع في أي بلدية و لو كان الممضي غير مقيم بالبلدية.

* يجب على المشتري التصريح بنقل ملكية مركبته خلال أجل شهر من تاريخ شطب بطاقة الترقيم طبقا للمادة 172 من المرسوم التنفيذي رقم 04-381 المؤرخ في 2004/11/28. في حالة تجاوز هذه المدة دون تحويل ملكية المركبة باسم المشتري يتعرض المشتري للغرامة المقدرة ب 2500 دج المنصوص عليها في المادة 66 (النقطة ب-9) من القانون رقم 17-05 المؤرخ في 16 فيفري 2017.

Figure 4Sales Permit Document :

Following this, the buyer proceeds to the registration office to submit an application file for a new vehicle registration card. As specified on the website of the Ministry of Interior, Local Authorities and Spatial Planning, the required documents include:

"The citizen must complete a vehicle registration application form, which can be obtained from the relevant municipal services or downloaded from the Ministry's official website. This form must be accompanied by the following documents for all vehicle registration requests:

- Residence card (except for vehicles belonging to foreign partners),
- Copy of the national identity card,
- Sales contract (except for new vehicles imported by individuals),
- Fiscal stamp duty payment,
- Vehicle transaction tax receipt (for taxable vehicles),
- Document confirming the buyer's legal status when the purchaser is a public or private legal entity."

Additionally, the canceled registration card must be included. If the vehicle was previously registered in a different province, the control card issued by the original province must be added to the file. Upon submission, the buyer receives a deposit receipt valid for one month, which can be used for subsequent procedures. [37]

الجمهوريـــــة الجزائريـــــة الديمقراطيـــــة الشعبيـــة

وزارة الداخلية و الجماعات المحلية و التهيئة العمرانية

استمارة طلب بطاقة ترقيم المركبات ذاتية الحركة

الولاية : الدائرة: البلدية :

الرجاء وضع علامة (x) في الخانة المناسبة

☐ ترقيم لأول مرة ☐ إعادة الترقيم ☐ تغيير مقر السكن لولاية أخرى ☐ نسخة ثانية ☐ تصحيح

☐ تغيير المواصفات التقنية للمركبة ☐ تغيير البيانات الخاصة (رفع الرهن، انتهاء التنازل، انتهاء مدة الإيجار...)

المركـــبـــة

رقم التسجيل الحالي | تاريخ إصدار بطاقة الترقيم الحالية | الرقم التسلسلي لبطاقة الترقيم | رقم التسجيل السابق

الصنف | الطراز | الرقم التسلسلي في الطراز

نوع المركبة | الهيكل | الطاقة

القوة | سنة أول وضع في السير | الحمولة الإجمالية المرخصة (PTAC) | الحمولة الإجمالية السائرة المرخصة (PTRA)

الحمولة المفيدة (CU) | عدد المقاعد (الجلوس) | عدد الواقفين

صاحـــب المركبـــة

☐ شخص طبيعي ☐ ذكر ☐ أنثى ☐ شخص معنوي

اللقب | الاسم | اللقب و الاسم بالحروف اللاتينية

الغرض الاجتماعي

ابن | و | الجنسية

ولد في | اليوم | الشهر | السنة | البلدية | الدائرة | الولاية | البلد

رقم التعريف الوطني | رقم السجل التجاري

العنوان | رقم الباب و/أو العمارة | طريق/ نهج/ جادة/ حي | قرية/ مشتة | بلدية | ولاية

أو المقر الاجتماعي

الرمز البريدي | رقم الهاتف | المهنة

المالكين المشتركين

الاسم و اللقب أو الغرض الاجتماعي

بيانـات خـاصة

☐ الرهن ☐ عدم التنازل ☐ إيجار ☐ مركبة تابعة لأجنبي ☐ سلك دبلوماسي و قنصلي ☐ بيانات أخرى

أصرح بشرفي عن صحة المعلومات الواردة في الاستمارة
كل تصريح كاذب من طرفي يعرضني للعقوبات المنصوص عليها في قانون العقوبات

حرر بـ

بتاريخ | اليوم | الشهر | السنة

الإمضاء

إطار مخصص للإدارة

اسم ولقب الموظف الذي استلم الملف

اسم ولقب الموظف الذي عاين الملف

ملاحظات هامة :

1. ملأ الاستمارة بكل وضوح و دقة لتفادي عدم قبولها من طرف الإدارة.
2. الاستمارة لا تخضع لعملية التصديق على الإمضاء.
3. يتم إثبات العنوان المذكور عن طريق وثيقة تبرر مقر الإقامة.

Figure 5 : New number card application form

Upon completing these steps, the buyer must wait between a few days to two weeks to receive the new registration card, which constitutes the final stage in the vehicle ownership transfer process.

Mandatory Technical Inspection

The technical inspection renewal is compulsory, as the law requires a comprehensive technical examination of the vehicle upon change of ownership, in accordance with Article 38 of Official Gazette No. 37 (2003).

As defined in Chapter 1 of the definitions section of Official Gazette No. 37:
"Technical inspection refers to the technical examination conducted to verify the vehicle's maintenance condition and its roadworthiness. The technical inspection may take the form of periodic inspection, non-periodic inspection, or counter-inspection as stipulated in the provisions of this decree."

Required Documents for Technical Inspection

Article 39 stipulates:
"During the vehicle technical inspection process, the vehicle owner must present to the technical inspector one of the following mandatory documents:

- The original registration card (carte grise) or a duplicate when applicable
- The receipt of registration card application submission."

Inspection Process and Outcomes

The buyer must visit an accredited technical inspection agency for this procedure. Following the inspection, Articles 43 and 44 specify that the buyer receives the following documents:

- Technical inspection report
- Inspection sticker, which must be immediately affixed to the lower left corner of the vehicle's windshield

According to Article 45, there are three possible inspection outcomes:

1. **Approved vehicle**: When no defects are noted by the inspector
2. **Rejected vehicle with driving prohibition**: Requires a counter-inspection after completing necessary repairs
3. **Rejected vehicle without driving prohibition**: Also requires a counter-inspection after completing repairs.[38]

2.3. Challenges Associated with the Traditional System

Algeria's conventional car ownership transfer system faces structural and procedural challenges that significantly impact the process's efficiency and reliability. The most prominent issues include:

1. **Cumbersome Paperwork**: Lengthy bureaucratic procedures result in extended processing times, failing to meet modern expectations of speed and efficiency in transactions.
2. **Administrative Burden**: Citizens must navigate multiple government offices (municipalities, tax authorities, technical inspection centers), creating fatigue and increasing the risk of document loss or errors.
3. **Fraud Vulnerabilities**: Buyers remain exposed to scams—whether through concealed vehicle defects or forged documentation—due to weak verification mechanisms.
4. **Market Inefficiencies**: Low liquidity in the used car secondary market prolongs sales cycles, making it harder for sellers to find trustworthy buyers.

The Path Forward
These systemic pain points highlight the urgent need for a secure intermediary system that:

- Protects both buyers' and sellers' rights
- Reduces dependence on physical paperwork
- Mitigates fraud risks through modern solutions like blockchain technology, which provides a decentralized, tamper-proof transaction ledger.

CHAPTER Three:

System Design – UML

3.1. Introduction

This chapter presents the system design using the Unified Modeling Language (UML). The diagrams were created using software that supports Arabic language to ensure clarity and accessibility for Arabic-speaking users.

To ensure the confidentiality of users' personal data, a layered encryption strategy is employed. Personal data is first encrypted using a symmetric encryption key. This key is then encrypted using the user's public key, and additionally encrypted using the public key of the governmental authority. This architecture ensures that only the authorized governmental entity and the respective user can access the sensitive information.

3.2. System Requirements (Functional and Non-Functional)

3.2.1. Functional Requirements

The functional requirements define the specific tasks the system must perform for its different stakeholders:

Technical Inspection Authority

Allow certified experts to add or update technical inspection reports for vehicles.

Link inspection reports to registered vehicles on the platform to ensure transparency.

Regular Use

Connect a Solana digital wallet to the platform to manage financial transactions

Submit account verification by uploading official identity documentation.

Browse listed vehicles with filtering and search features (e.g., by price, type, or location).

Create, update, or delete vehicle sale advertisements, including technical specifications.

Send and receive purchase offers, and accept or reject offers from other users.

Request detailed technical information about listed vehicles.

Execute purchases and transfer vehicle ownership through smart contracts on the Solana blockchain.

Government Authority

Digitally tokenize vehicles and associate them with their owners in a centralized blockchain registry.

Verify the accounts of regular users and certified entities (e.g., Technical Inspection Authority and Mining Compliance Expert)

Mining Complianc Expert

Add technical compliance certificates for vehicles to the blockchain, verifying their legal conformity.

3.2.2. Non-Functional Requirements

These requirements specify the quality attributes necessary to ensure the system's performance, security, and usability.

Security

All sensitive data (e.g., personal identity and official documents) must be encrypted using strong encryption algorithms such as AES-256.

Encrypted data must be stored on the decentralized IPFS network to ensure data privacy and integrity.

Access to sensitive governmental data must be restricted to authorized entities using controlled encryption keys managed by the responsible authority.

The system must comply with security best practices for Solana-based applications, including proper transaction verification and signing via supported wallets.

Access to technical inspection data must be limited to the concerned user and the governmental authority

Data Integrity

Official documents (e.g., inspection reports, ownership certificates) must be stored on IPFS to guarantee immutability.

Each ownership document must be linked to a unique hash recorded on the blockchain to enable authenticity verification.

Usability

The user interface must support both Arabic and English languages.

Interactive guides or tooltips should be available to explain how to perform actions such as wallet connection, car purchase, and advertisement posting

The platform should be user-friendly and accessible to individuals with limited technical background.

3.3. Use Case Diagram

The use case diagram illustrates the interactions between the system and its primary actors, highlighting the main functionalities available to each.

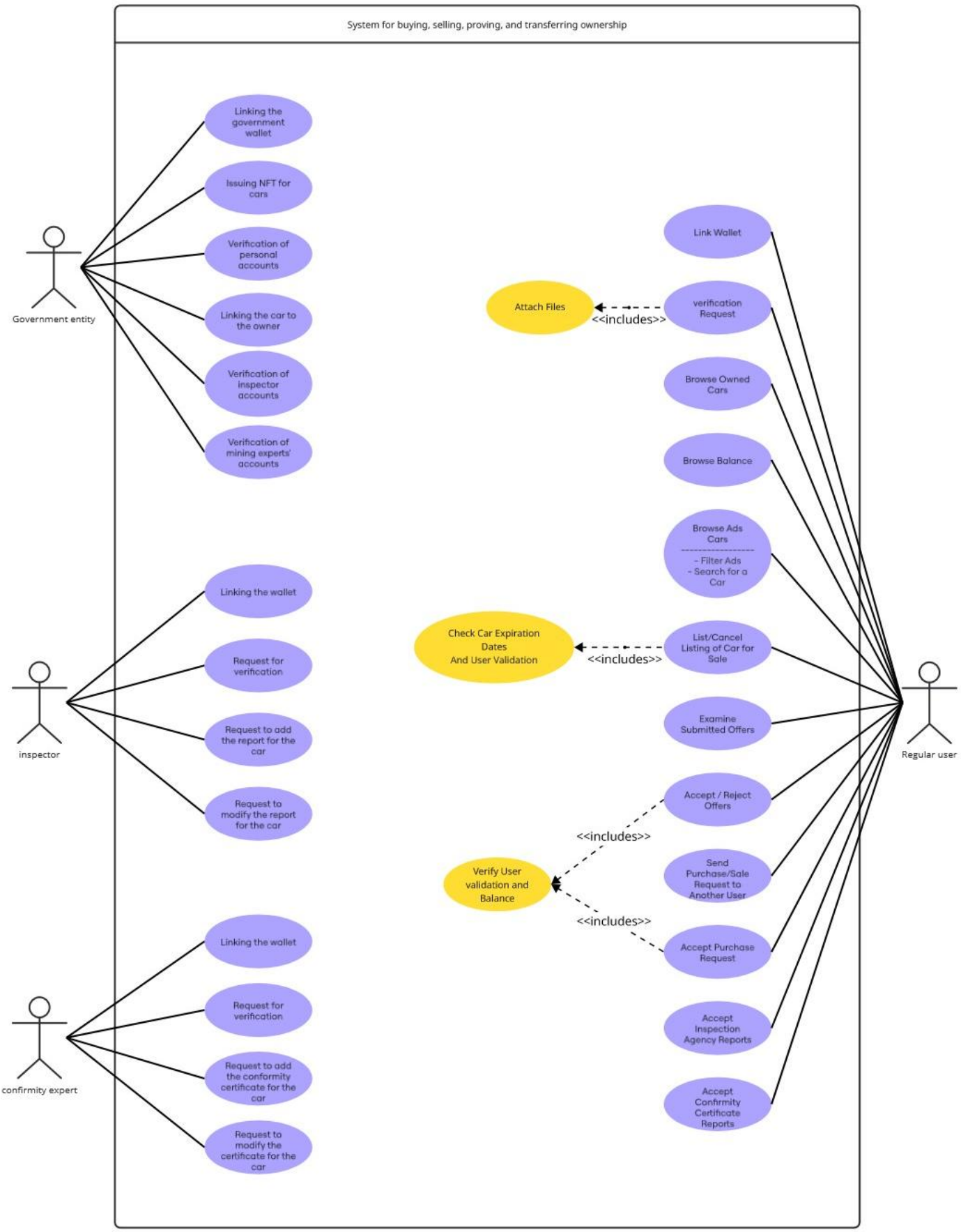

Figure 6 :Use Cases Diagram

3.4. Sequence Diagram

The sequence diagram depicts the flow of interactions and data between users, system modules, and external components (e.g., blockchain and IPFS) during key processes such as purchasing and inspection submission.

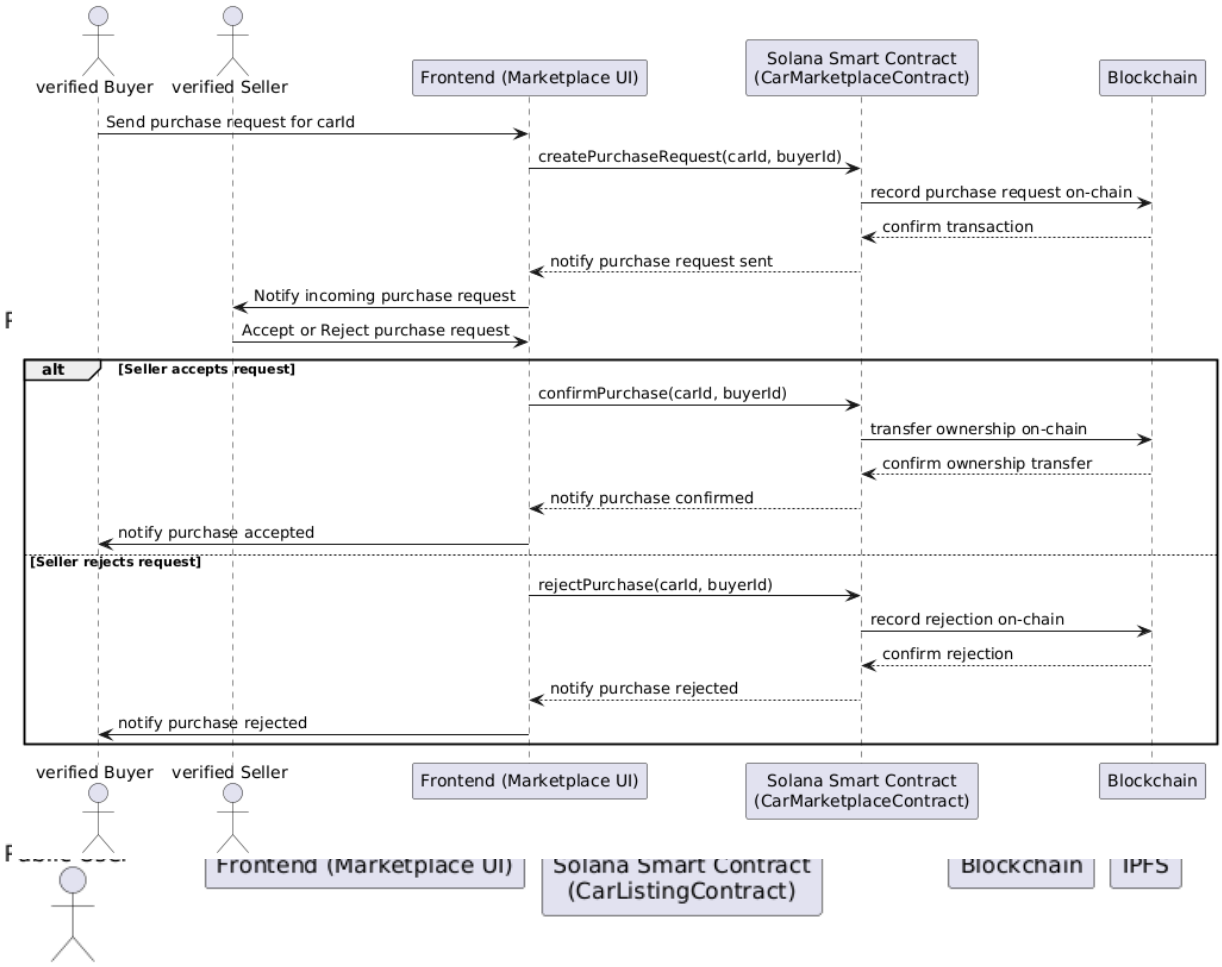

Figure 7 :List Car NFT Squence Diagram

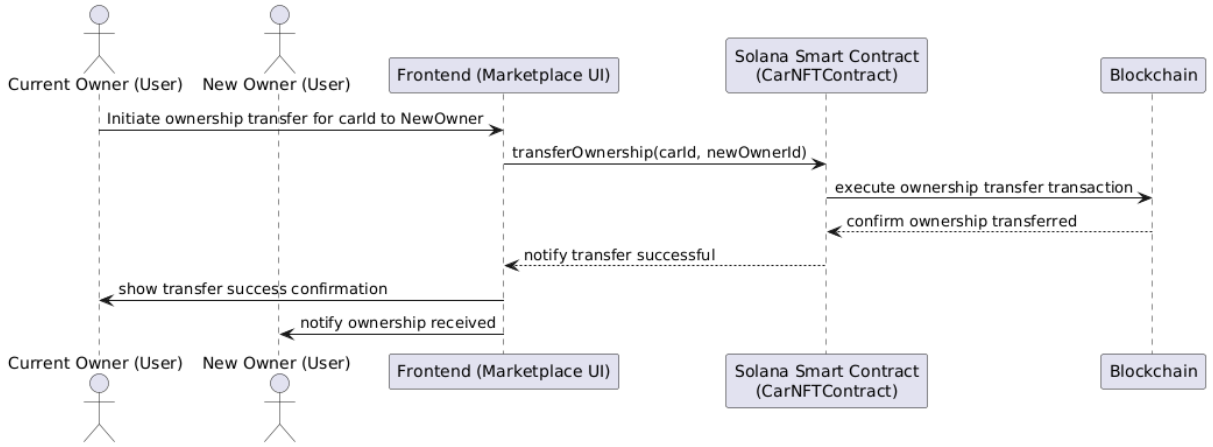

Figure 9 Transfer OwnerShip Squence Diagram

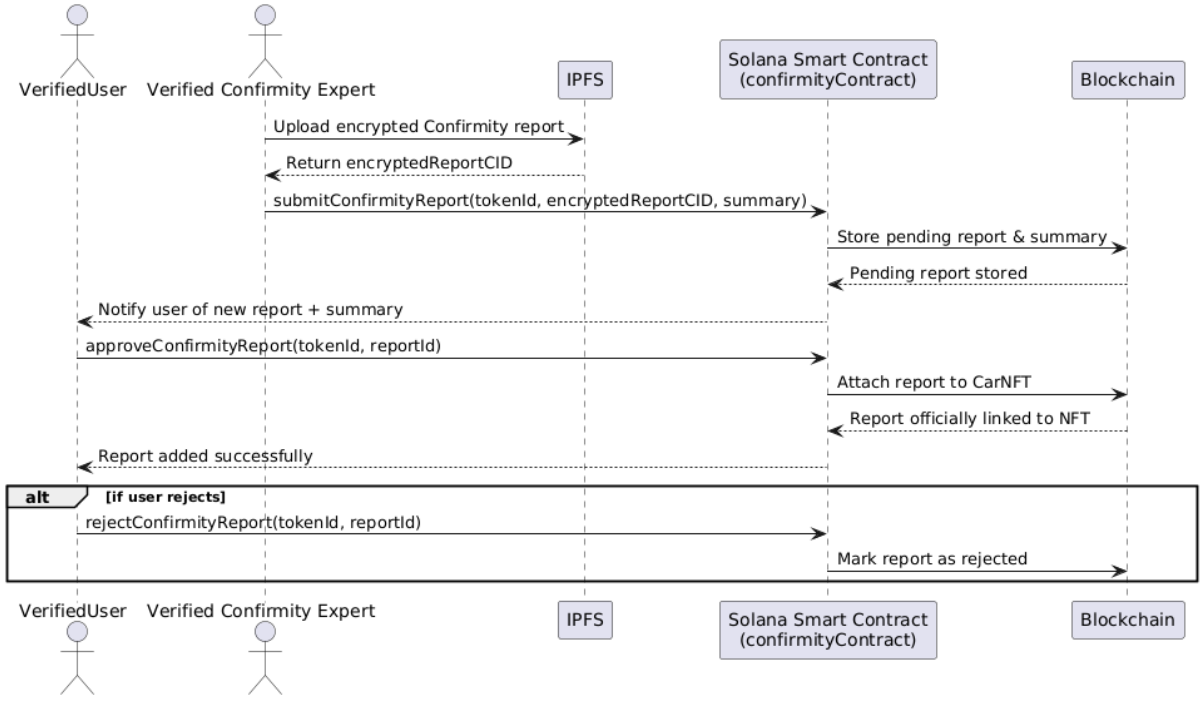

Figure 8 Conformity Sequence diagram

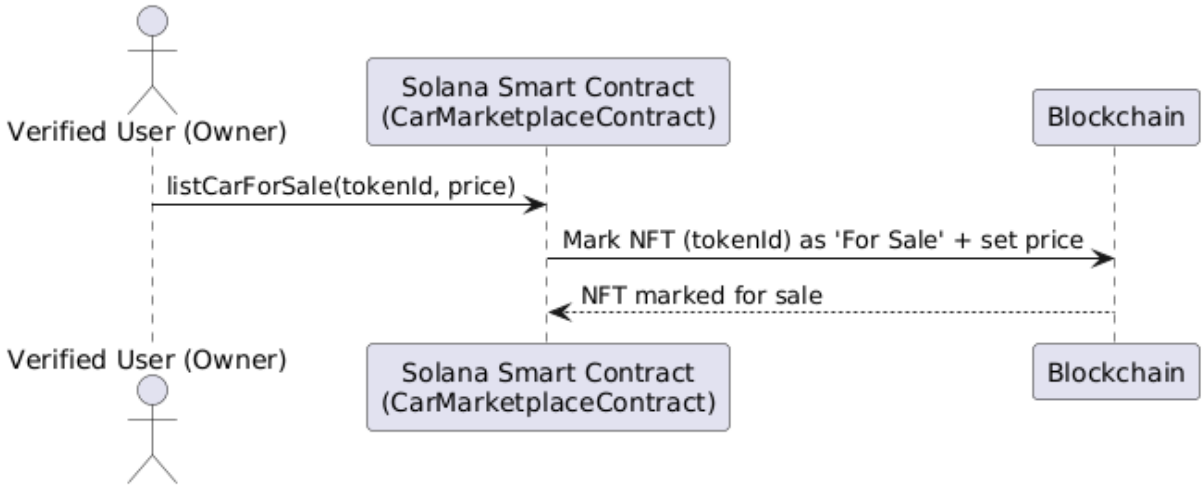

Figure 10 set nft for sale sequence diagram

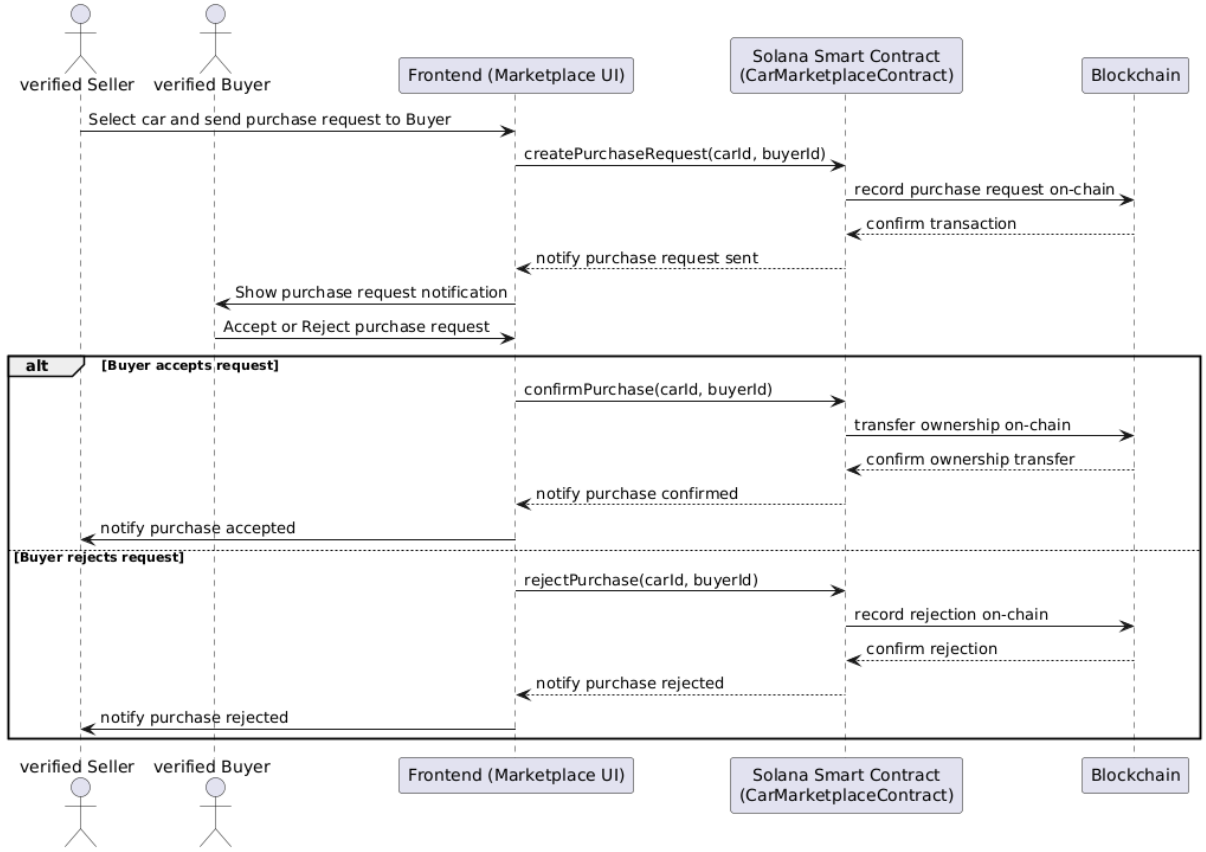

Figure 11 buy car nft Sequence Diagram

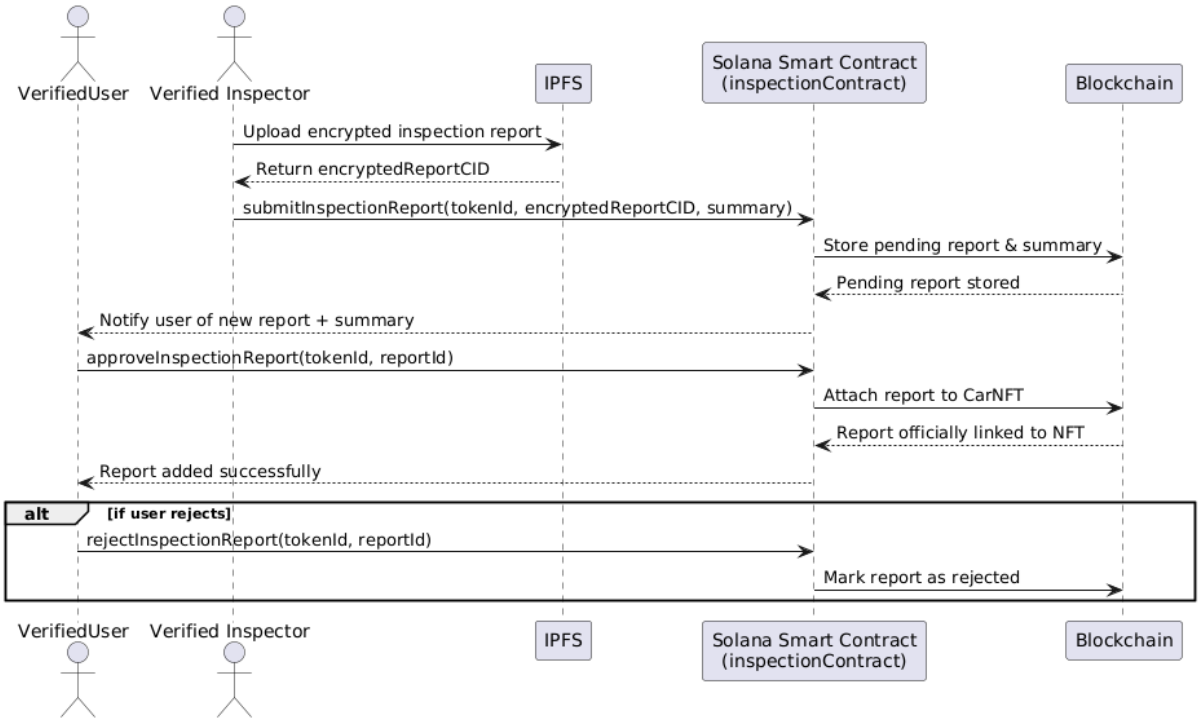

Figure 13 Inspector Sequence diagram

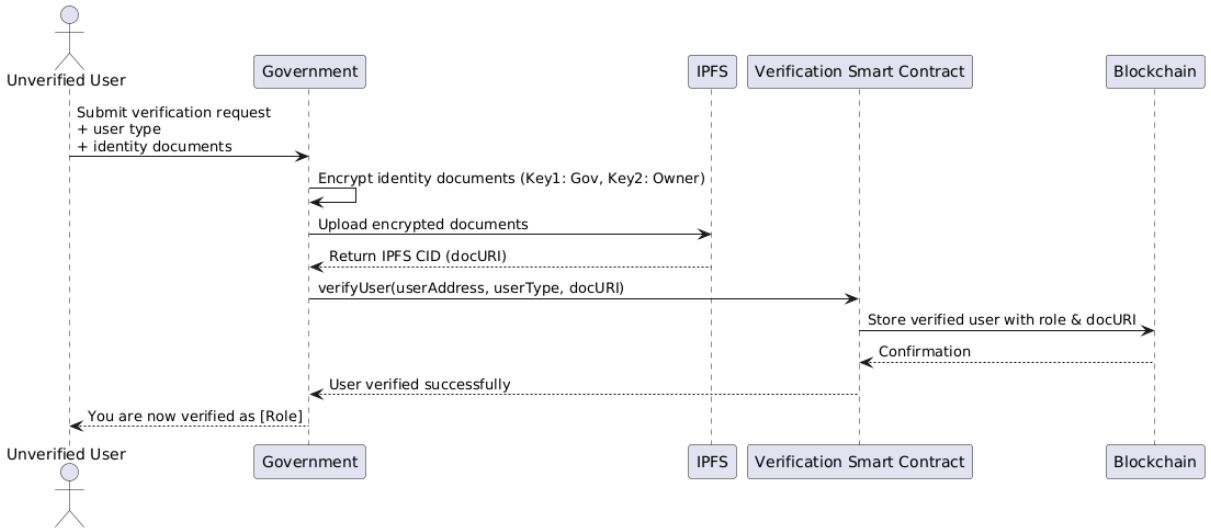

Figure 12 Verify users sequence diagram

3.5. Class Diagram

The class diagram defines the system's data structure, including classes, attributes, and relationships. Metadata stores detailed object information, while sensitive data is encrypted and stored in IPFS to ensure secure and decentralized access.

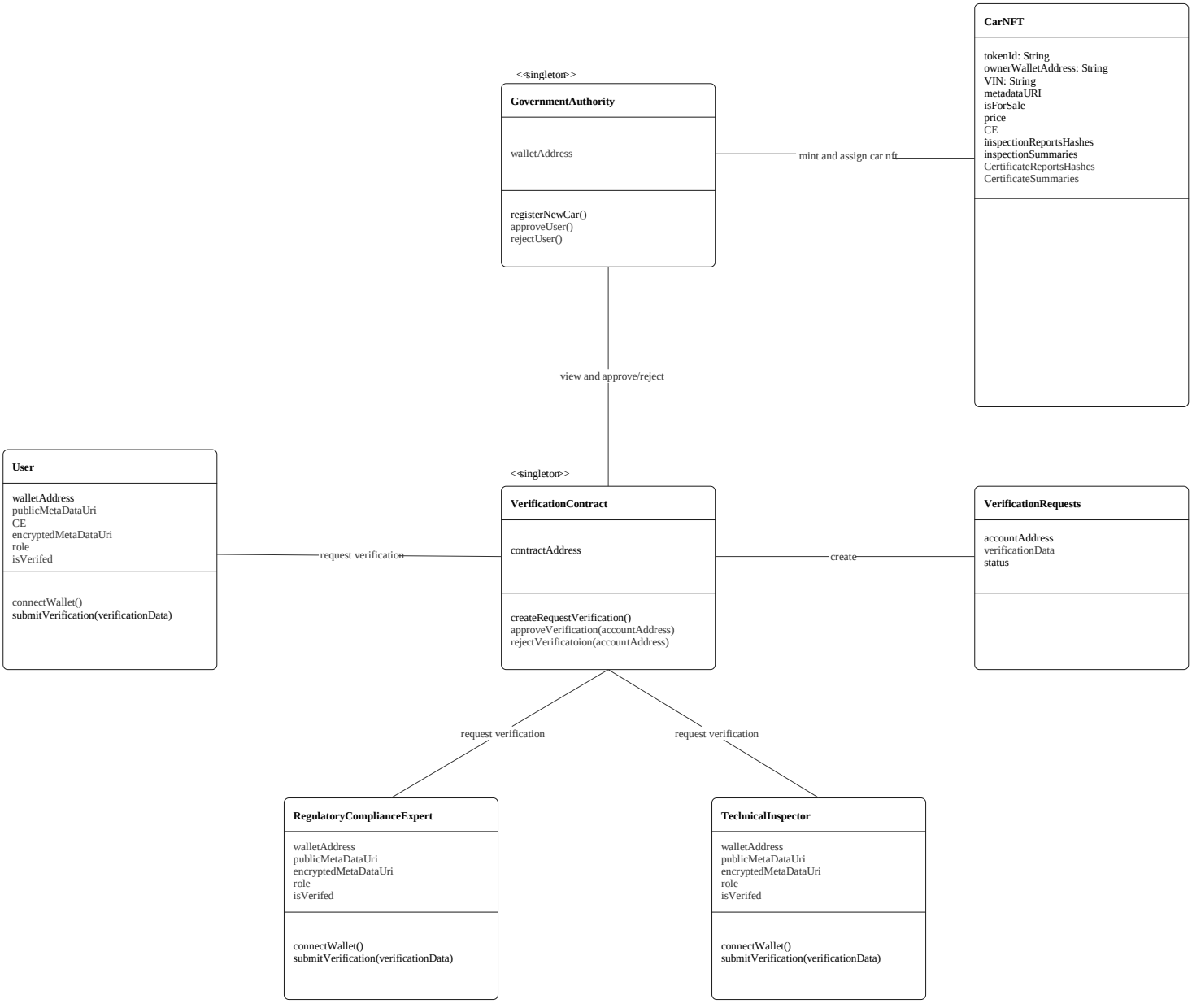

Figure 14 : government related class diagram

Inspector package - class diagram

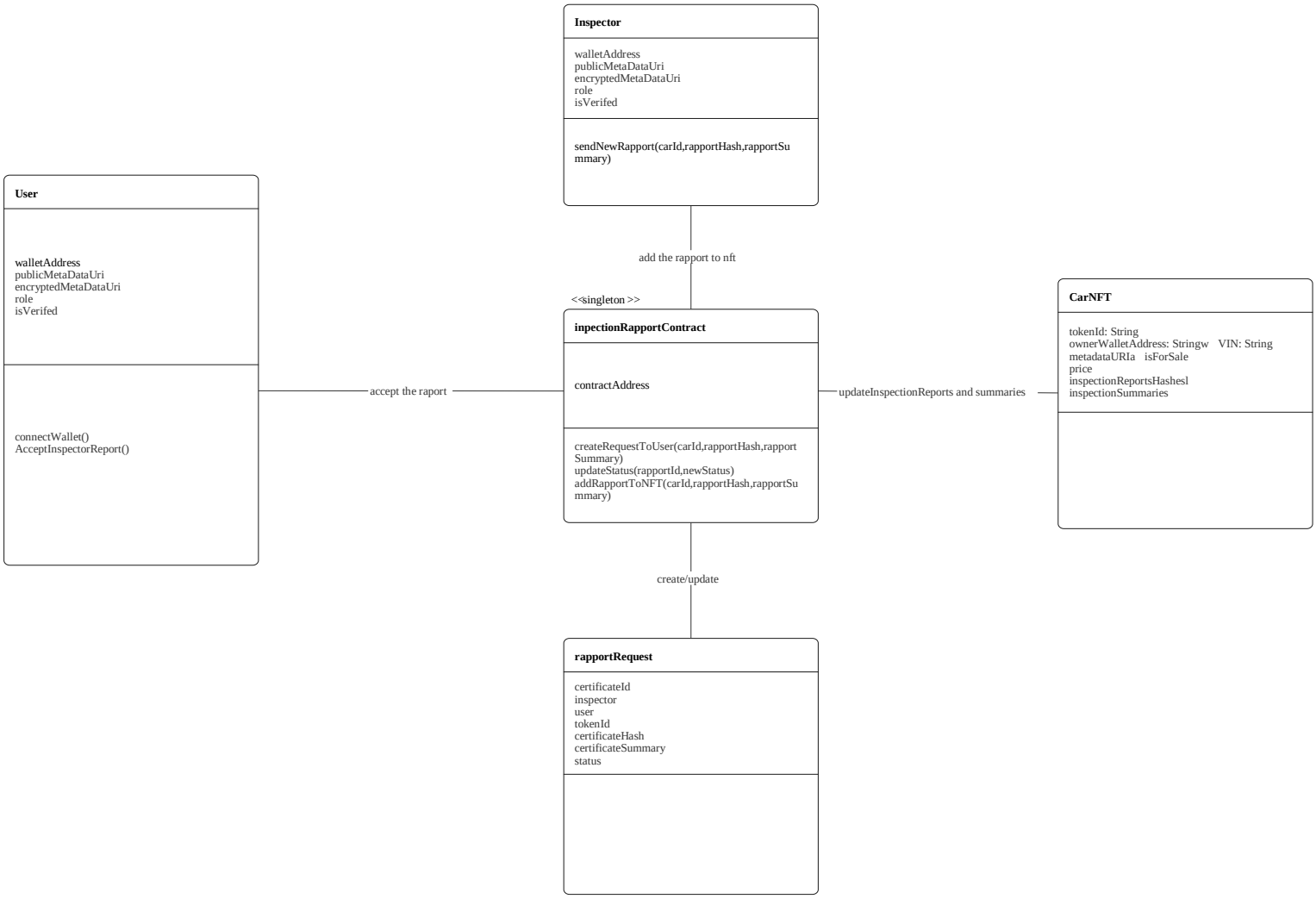

Figure 15 : Inspector related class diagram

Conformity package - class diagram

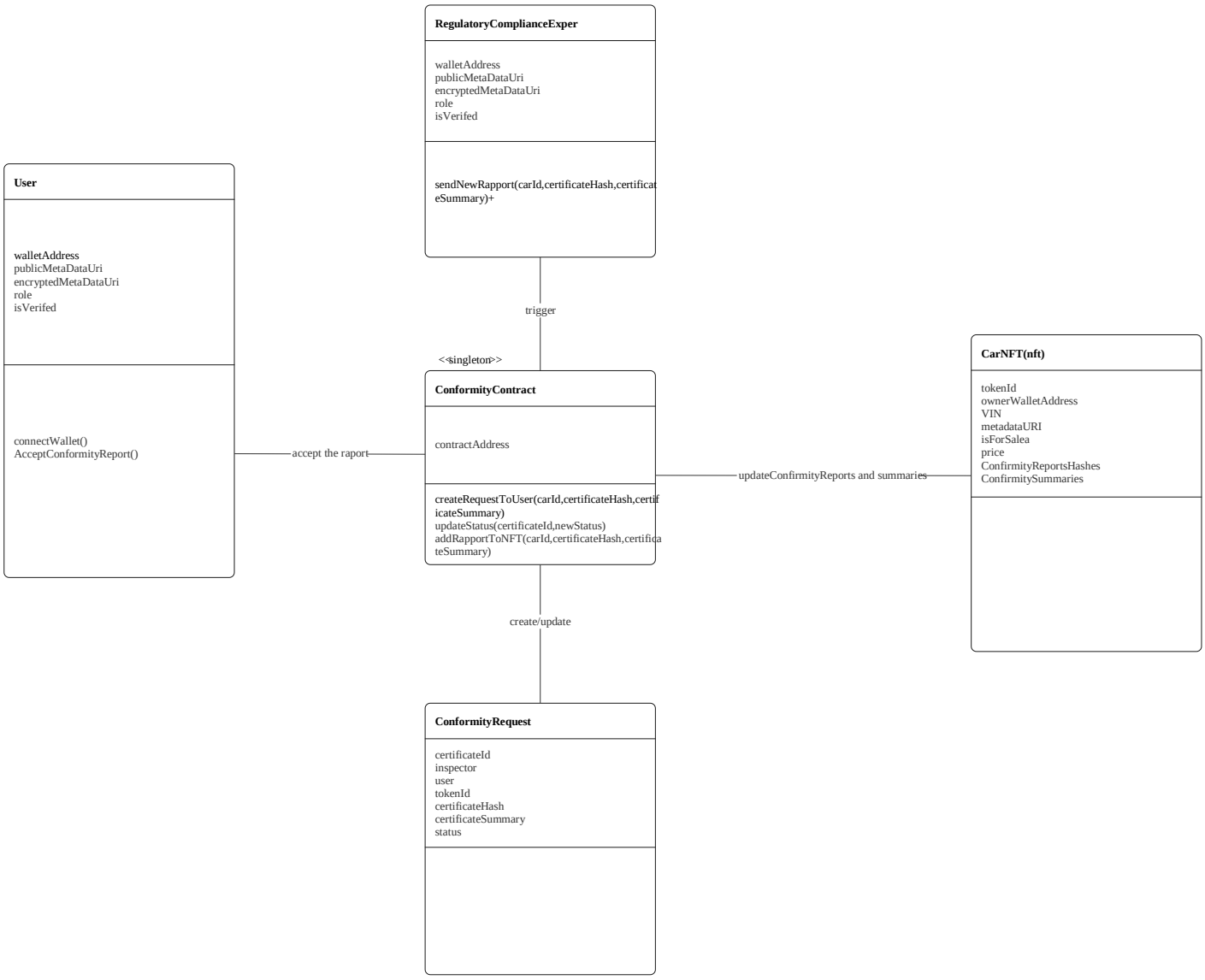

Figure 16 :Conformity Expert - class diagram

Marketplace package - class diagram

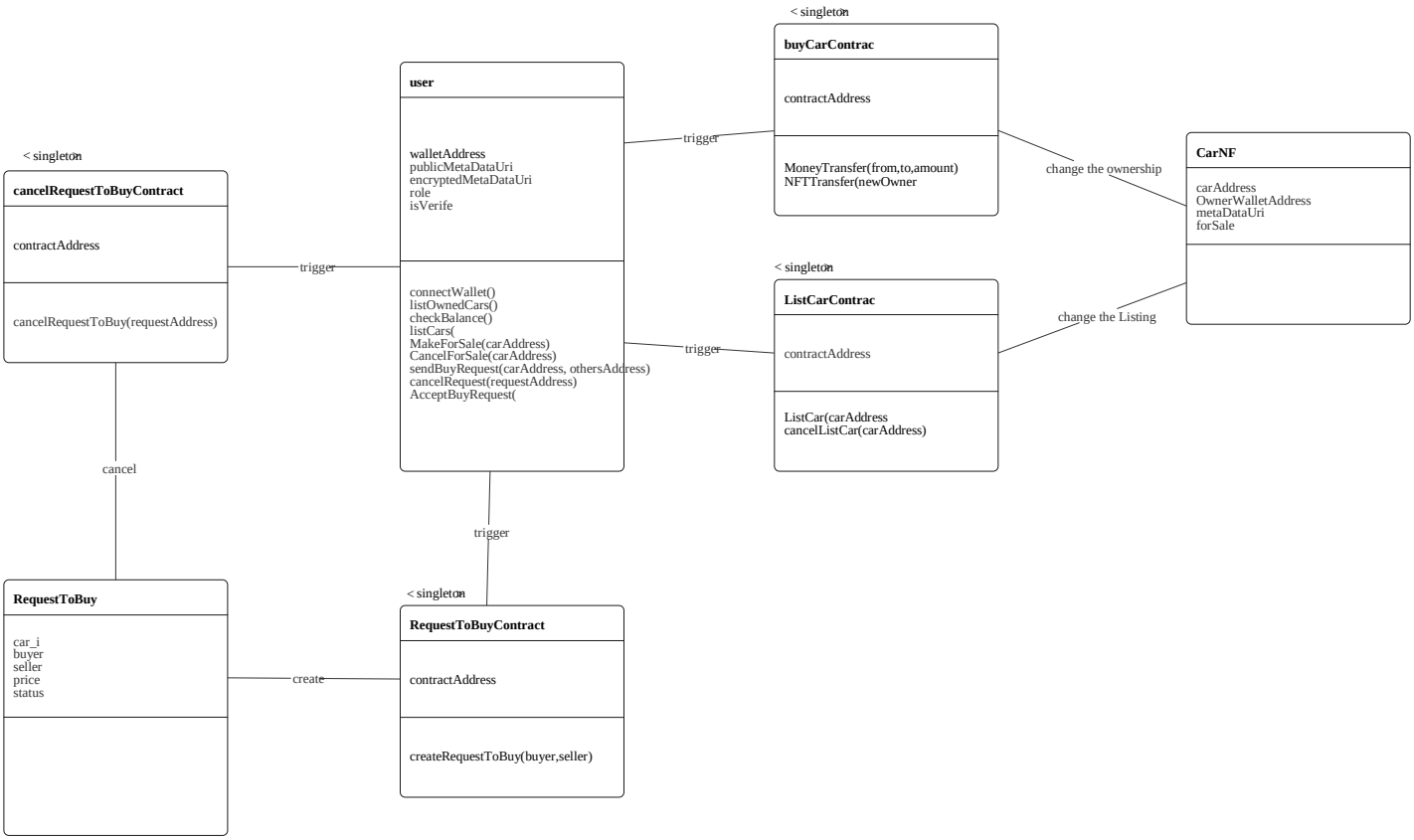

Figure 17 :Marketplace related class diagram

3.6. Deployment Diagram

The deployment diagram illustrates the physical system architecture, showing components such as the user interface, backend services, blockchain network nodes, IPFS storage, and secure communication protocols connecting them.

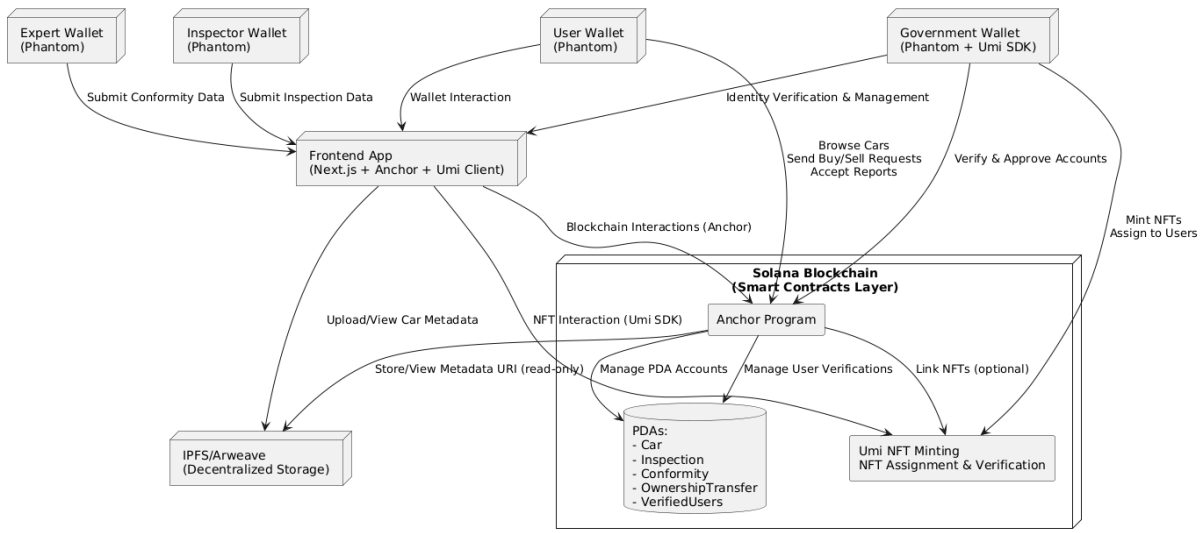

Figure 18 deployment diagram

Ownership package - class diagram

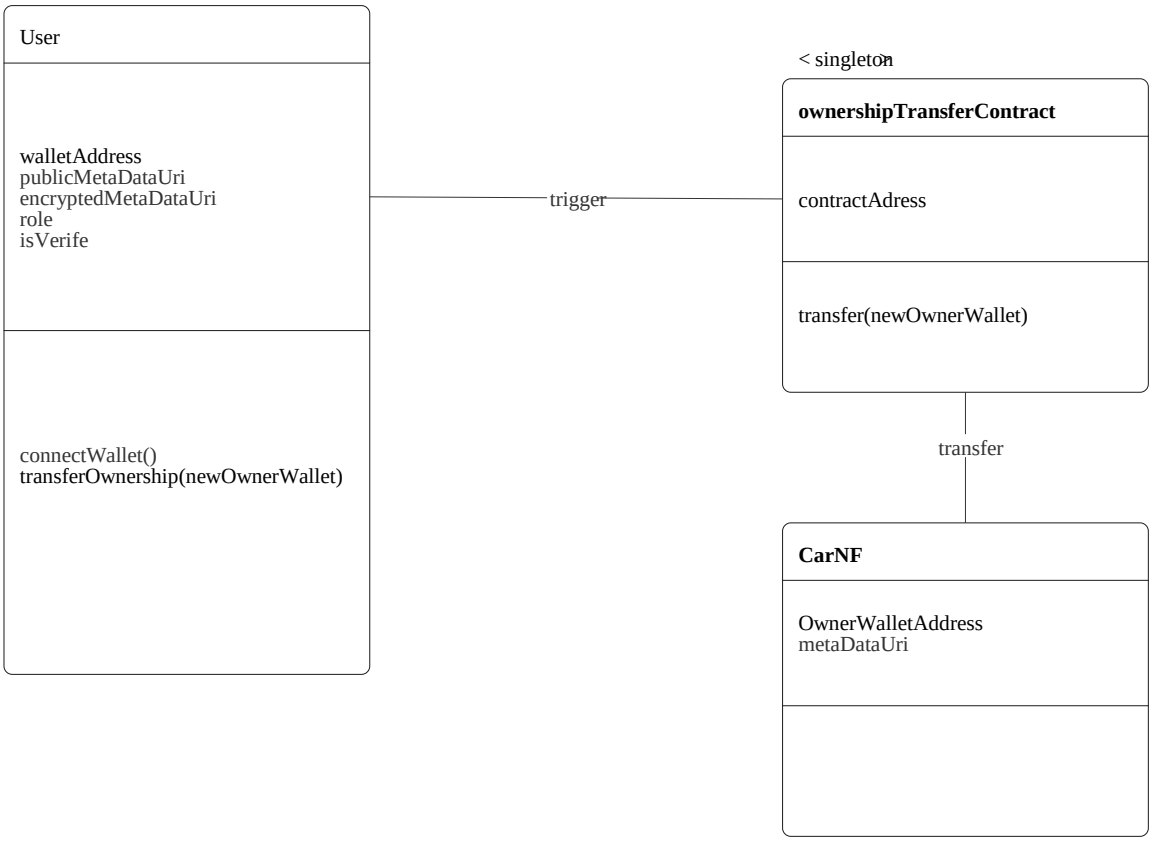

Figure 19 : Owner ship related class diagram

Chapter five :

Implementation

4.1. Introduction

This chapter presents the implementation of Platform, trying to follow the system design and UML diagrams from Chapter 4. The implementation realizes a blockchain-based system for managing car ownership, sales, and inspection reports using modern web technologies integrated with Solana blockchain.

4.2. Technology Stack

The implementation utilizes the following at the first place ready made template from solana team and this template use this technology stack:

Blockchain Layer:

- Solana blockchain platform
- Anchor framework (Rust-based) - started from official template
- Smart contracts for business logic

Frontend Layer:

- Next.js with TypeScript
- Tailwind CSS + DaisyUI for styling
- Framer Motion for animations
- Lucide React for icons
- TanStack Query for state management

Integration Layer:

- Solana Web3.js for blockchain interaction
- Anchor client for smart contract communication
- Phantom wallet integration

4.3. Smart Contract Implementation

Building upon the Anchor template, the smart contracts implement the core business logic through various instruction handlers:

4.3.1. Program Structure

```
// Core instruction modules - built upon template structure
pub mod register_user;
pub mod verify_user;
pub mod register_car;
pub mod transfer_car;
pub mod issue_car_report;
pub mod accept_buy_request;
```

4.3.2. Key Instructions

Car Registration Implementation:

```
// register_car.rs - Extended from template instruction handler
pub fn handler(
    ctx: Context<RegisterCar>,
    car_id: u64,
    vin: String,
    brand: String,
    model: String,
    year: u16,
    // ... other parameters
) -> Result<()> {
    // Validation logic
    require!(!vin.is_empty() && vin.len() == 17, CarError::InvalidVin);
    require!(!brand.is_empty() && brand.len() <= 30, CarError::InvalidBrand);
```

```
    require!(year >= 1900 && year <= 2025, CarError::InvalidYear);

    let car = &mut ctx.accounts.car;
    let clock = Clock::get()?;

    // Initialize car data
    car.car_id = car_id;
    car.vin = vin;
    car.brand = brand;
    car.model = model;
    car.year = year;
    car.owner = owner;
    car.registered_by = ctx.accounts.government.key();
    car.registration_date = Some(clock.unix_timestamp);
    car.is_active = true;

    Ok(())
}
```

Car Transfer Implementation:

```
pub fn handler(ctx: Context<TransferCar>, vin: String, user_name: String) -> Result<()> {
    let car = &mut ctx.accounts.car;

    // Verify current owner
    require!(
        car.owner == ctx.accounts.current_owner.key(),
        CarError::UnauthorizedAccess
    );

    // Verify new owner is verified
    require!(
        ctx.accounts.new_owner_pda.verification_status == VerificationStatus::Verified,
```

```
            CustomError::UserNotVerified
        );

        // Execute transfer
        car.owner = ctx.accounts.new_owner.key();
        car.transfer_count += 1;

        Ok(())
}
```

Inspection Report Creation:

```
pub fn handler(
        ctx: Context<IssueCarReport>,
        report_id: u64,
        vin: String,
        overall_condition: u8,
        engine_condition: u8,
        body_condition: u8,
        full_report_uri: String,
        report_summary: String,
        notes: String,
) -> Result<()> {
        // Validate input data
        require!(overall_condition >= 1 && overall_condition <= 10,
                CarReportError::InvalidConditionScore);
        require!(engine_condition >= 1 && engine_condition <= 10,
                CarReportError::InvalidConditionScore);
        require!(body_condition >= 1 && body_condition <= 10,
                CarReportError::InvalidConditionScore);
        require!(notes.len() <= CarReport::MAX_NOTES_LENGTH,
                CarReportError::NotesTooLong);
```

```
    let report = &mut ctx.accounts.car_report;

    // Initialize report
    report.car_vin = vin;
    report.overall_condition = overall_condition;
    report.engine_condition = engine_condition;
    report.body_condition = body_condition;
    report.full_report_uri = full_report_uri;
    report.report_summary = report_summary;
    report.notes = notes;
    report.status = ReportStatus::PendingApproval;

    Ok(())
}
```

4.4. Frontend Implementation

Building upon the Solana dApp template, the frontend implements a responsive web application with modern UI/UX principles:

4.4.1. 3.3. Marketplace Interface

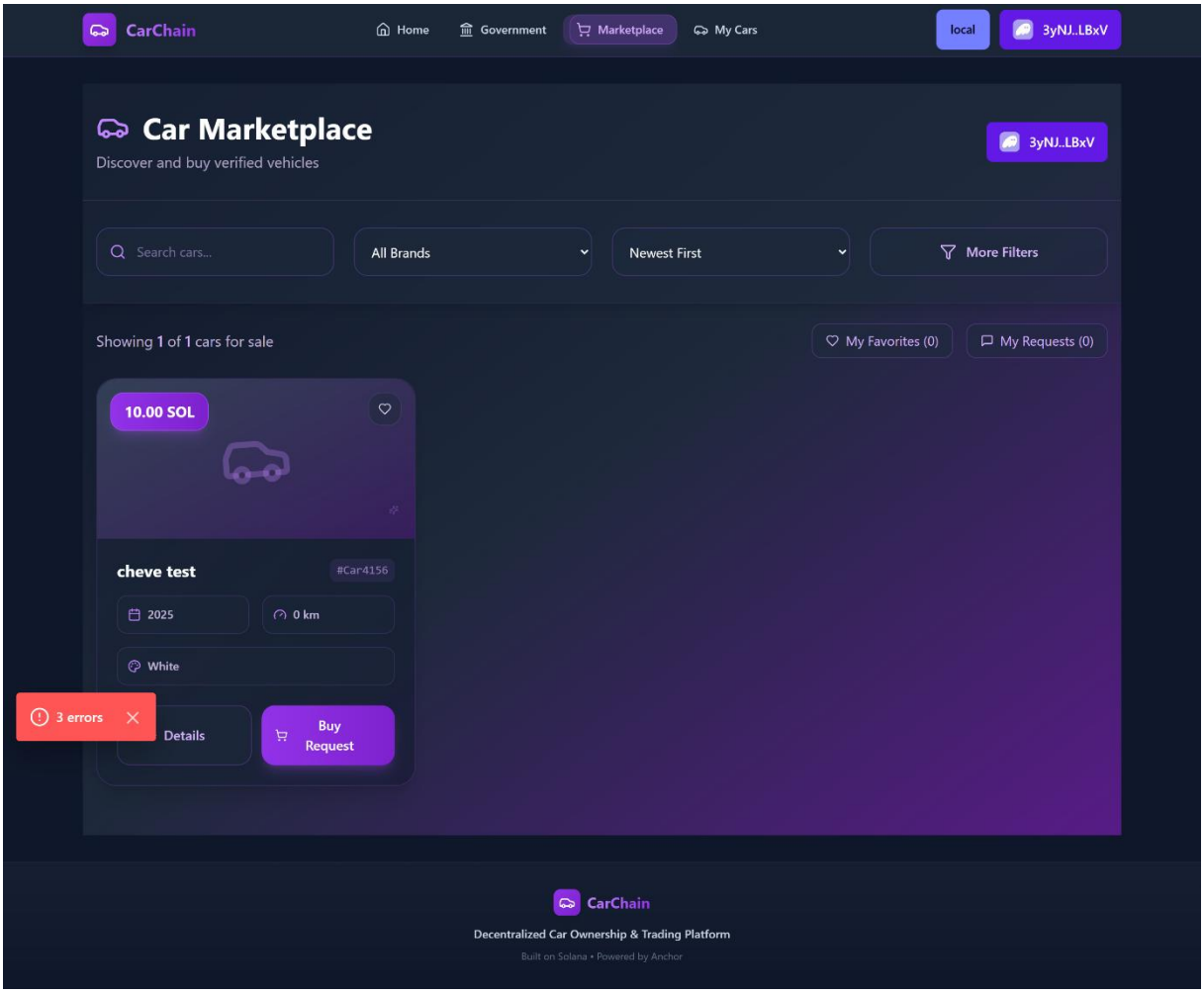

Figure 20 Car MarketPlace Page

4.4.2. Inspection Report Interface

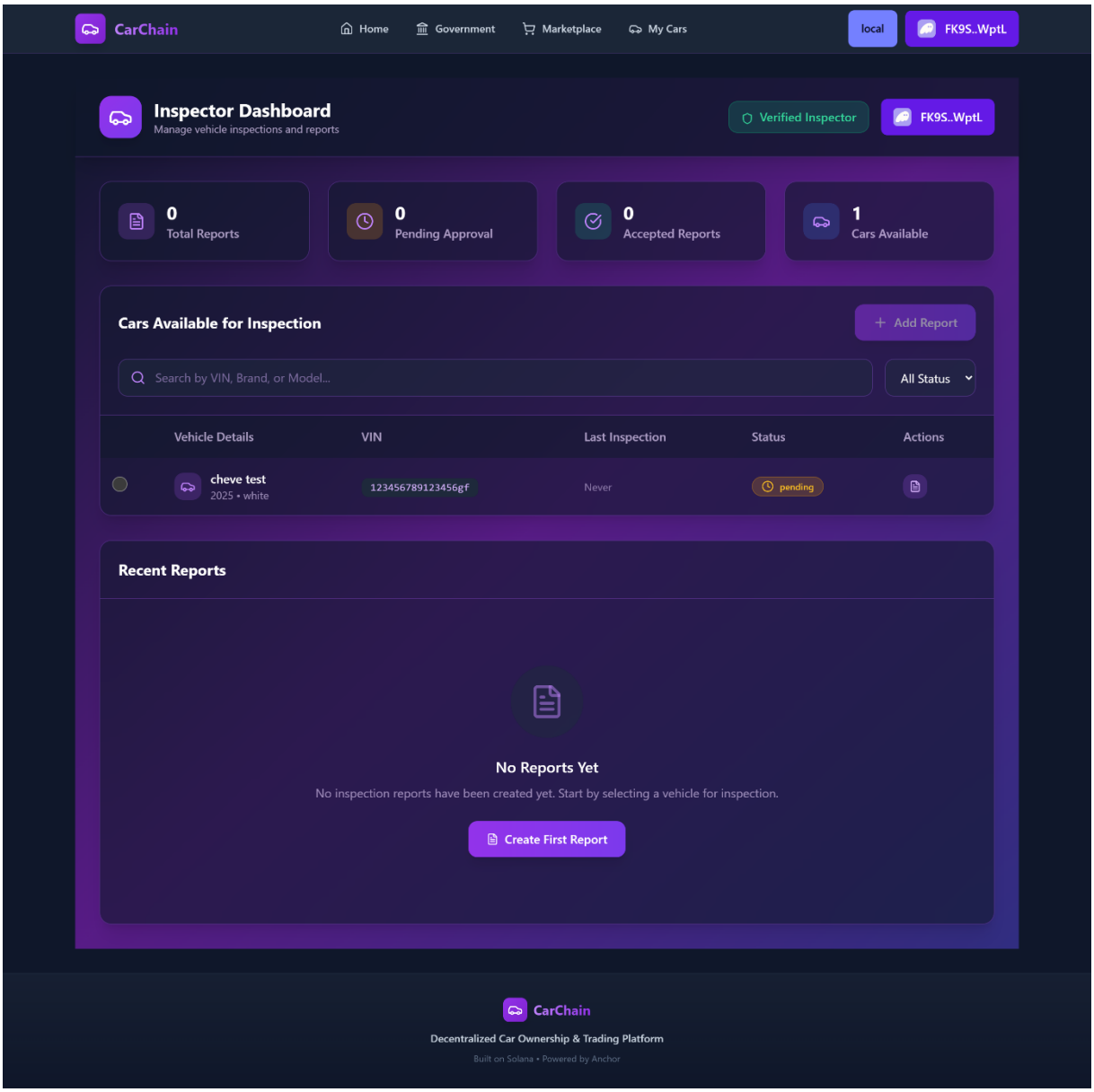

Figure 21 Inspector Interface

4.4.3. Conformity Dashboard

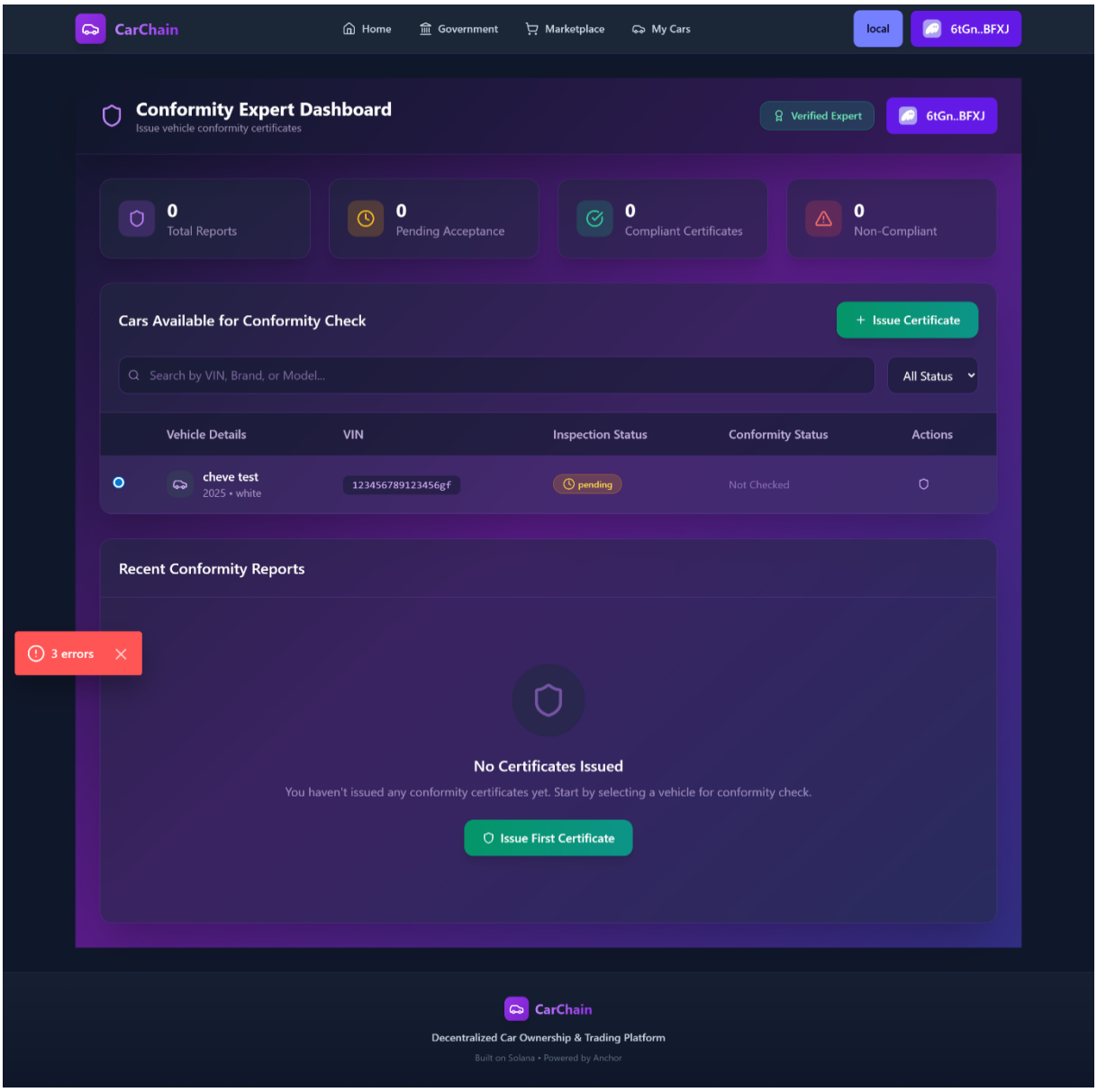

Figure 22 Conformity Expert Dashboard

Comprehensive transaction tracking with status updates, history, and detailed transaction information.

4.4.4. 3.6. Government Dashboard

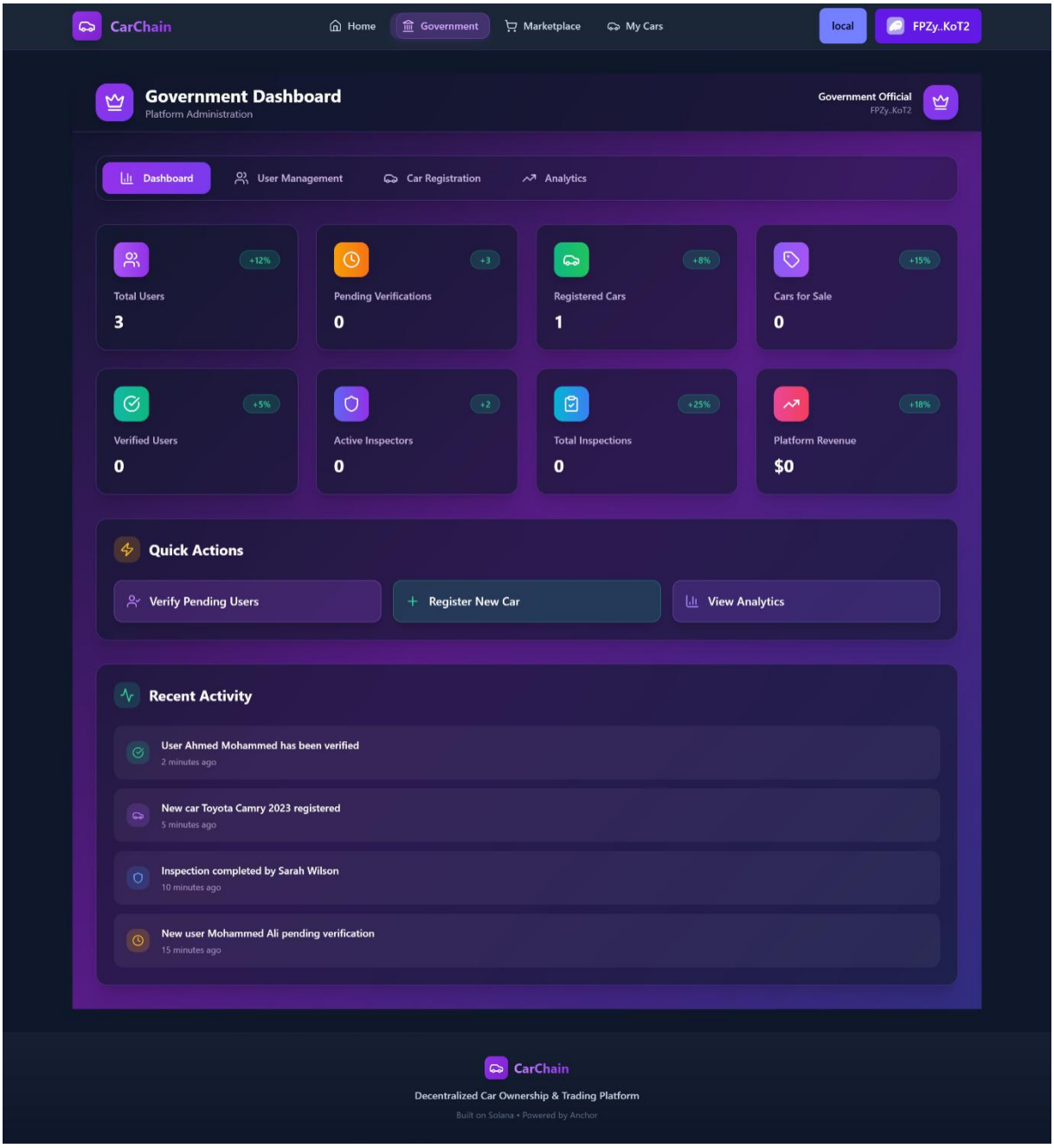

Figure 23 main dashboard

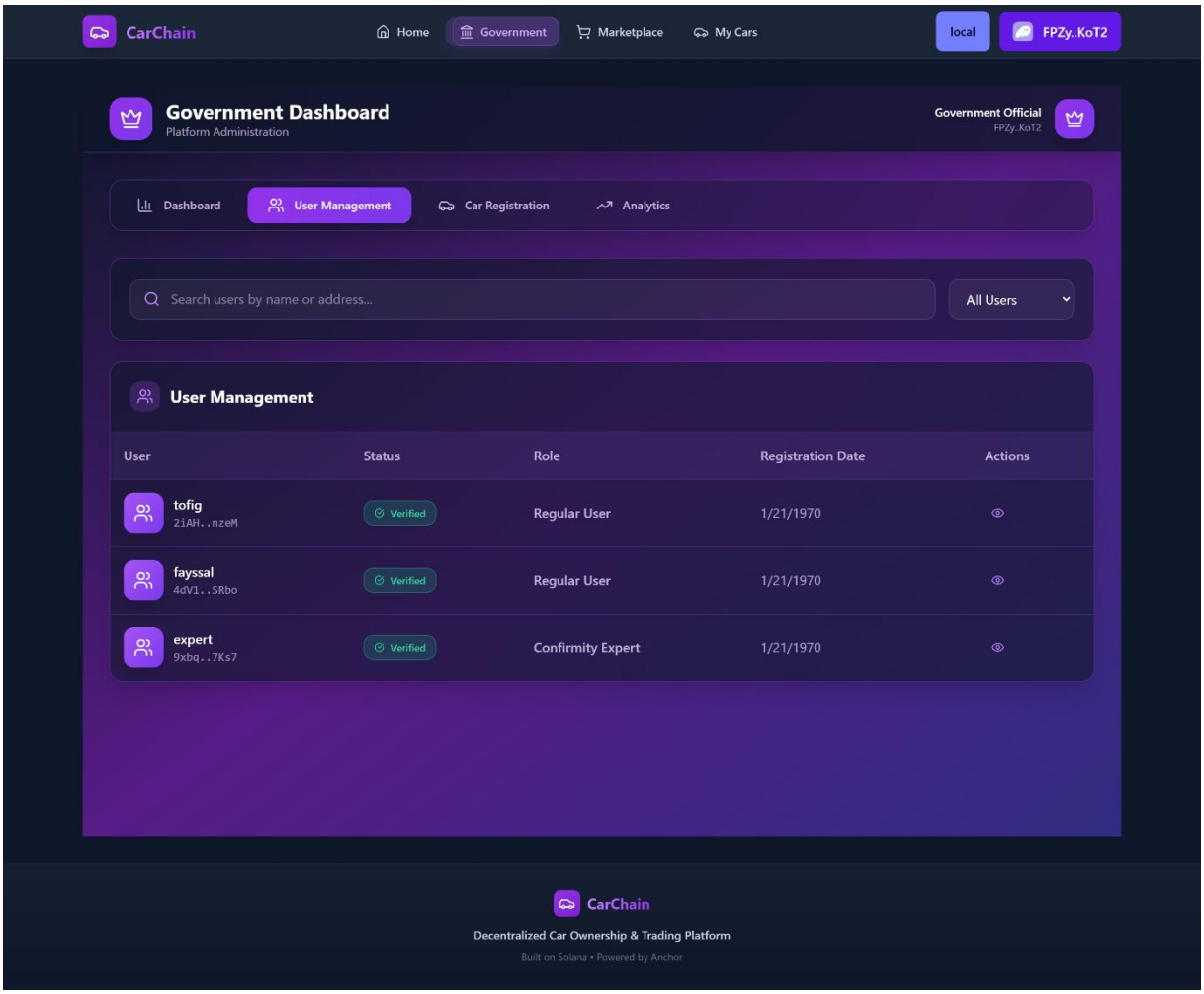

Figure 24 User Management

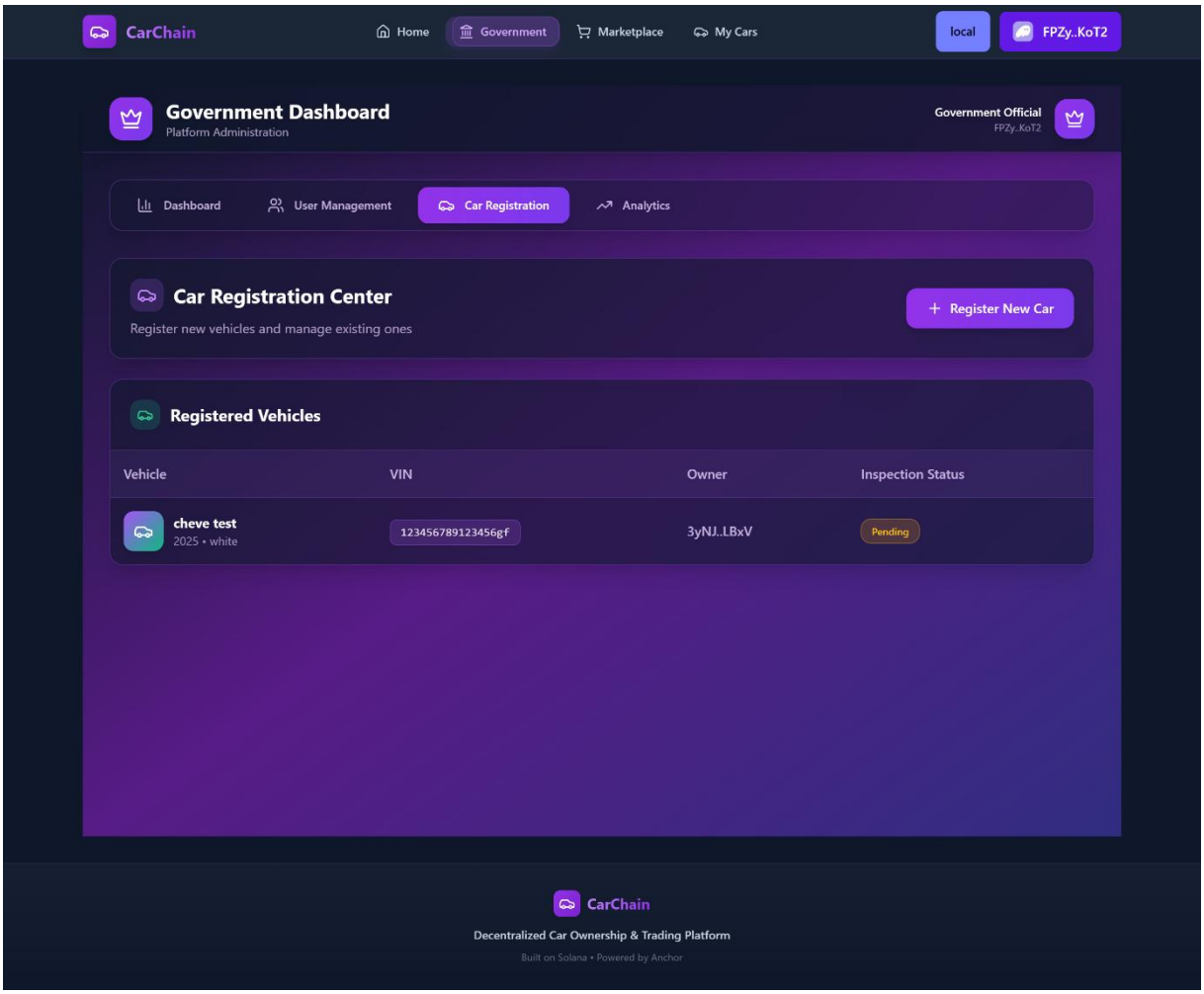

Figure 25 Car Registration Center Tab

4.4.5. Deployment

The system is deployed on Solana's localnet for testing with the frontend hosted locally. The smart contracts are deployed using Anchor CLI, while the frontend runs on Next.js and use par default nx mono repo.

And before deploy it you should use wsl and run solana-test-validator .

Smart contract deployment

anchor build

anchor deploy --provider.cluster localnet

Frontend development server

npm run dev

CHAPTER SIX :

Challenges and Futures Implementation

5.1. Legal Challenges

5.1.1. Legal Recognition of Cryptocurrencies:

- **Recognition of Cryptocurrencies as Legal Tender**
  Despite the growing integration of cryptocurrencies into modern economic discourse, the majority of sovereign governments refrain from acknowledging them as official legal tender. Bitcoin, Ethereum, and similar digital assets, although widespread in use, remain outside the boundaries of state-sanctioned currency systems — with a few notable exceptions, such as El Salvador and the Central African Republic, where regulatory frameworks have taken a divergent path.
  This regulatory hesitancy has practical implications: for instance, even if a transactional agreement — say, the purchase of a vehicle — is executed using crypto assets, the legal machinery governing title transfer may still necessitate documentation in fiat currency. Thus, cryptocurrency, while functionally operative, often finds itself legally invisible in key procedural moments.

- **Taxation and Financial Reporting Obligations**
  In many jurisdictions — the United States, United Kingdom, Canada, and the broader European Union among them — cryptocurrencies are not treated as currency per se but rather as property or assets subject to capital gains taxation. This classification implies that any disposal event, whether through exchange or sale, could constitute a taxable moment, triggering reporting requirements and potential liabilities.
  Furthermore, an additional layer of complexity arises in regions that extend sales tax or value-added tax (VAT) obligations to crypto transactions. These policies, still under refinement in many nations, reflect the broader challenge of fitting a decentralized digital phenomenon into the traditional tax mold — an uneasy fit, much like forcing digital water through analog pipes.

- **c) Regulatory Constraints in Banking and Financial Institutions**
  A persistent tension exists between the decentralized ethos of cryptocurrencies and the conservative mechanisms of traditional banking. Numerous financial institutions continue to regard crypto-linked transactions with skepticism, often designating them as high-risk and subjecting associated accounts to freezes or enhanced scrutiny — sometimes preemptively and with little transparency.
  In parallel, applications or platforms that enable the conversion of crypto into fiat currency may be obligated to secure specific regulatory credentials, such as a Money Transmitter License (MTL) or its equivalent. The necessity for such licensure underscores the state's enduring role as gatekeeper to monetary legitimacy, even as digital finance evolves around — and sometimes in spite of — it.

5.1.2. Government Reliance on Crypto Platforms:

- **Adherence to Anti-Money Laundering (AML) and Know Your Customer (KYC) Frameworks**
  Contemporary regulatory landscapes increasingly impose stringent requirements on cryptocurrency service providers to comply with Anti-Money Laundering (AML) and Know Your Customer (KYC) regulations. For instance, under the European Union's Markets in Crypto-Assets (MiCA) Regulation and the Financial Crimes Enforcement Network (FinCEN) guidelines in the United States, platforms facilitating digital asset transactions are obligated to authenticate user identities through formal documentation processes.
  Moreover, applications that facilitate high-volume or high-risk transfers may encounter legal imperatives mandating the collection of personal identification records. This requirement is not merely procedural but a safeguard against systemic misuse — albeit one that challenges the anonymity ethos underpinning blockchain technology.

- **Tensions with Central Bank Digital Currency (CBDC) Initiatives**
  As several states accelerate the development and deployment of Central Bank Digital Currencies (CBDCs), such as the proposed Digital Euro or Digital Dollar, a competitive dynamic emerges between state-backed digital currencies and privately-issued cryptocurrencies. In the name of regulatory clarity or systemic control, governments may enact policies that constrain the utility or legal viability of decentralized alternatives. This strategic prioritization of CBDCs introduces a latent risk for private-sector developers: future legislative action might restrict or outright prohibit certain types of crypto transactions, thereby potentially undermining the operational continuity of applications dependent on such mechanisms.

- **Legal Ambiguity Surrounding Smart Contracts**
  Smart contracts, particularly those employed within decentralized finance (DeFi) protocols or escrow arrangements, exist in a legal gray area in many jurisdictions. While these self-executing contracts offer efficiency and automation, their enforceability in traditional legal systems remains uncertain.
  To mitigate such legal fragility, developers are advised to supplement smart contract logic with conventional written agreements, thereby establishing an enforceable framework in the event of disputes or unforeseen transactional breakdowns. This dual-contract model, though redundant in appearance, serves as a legal anchor in environments where code alone lacks juridical recognition.

5.2. Security Challenges

5.2.1. Key Management & Digital Wallet Risks :

5.2.1.1. Risk of Losing Private Keys

One of the critical vulnerabilities in cryptocurrency systems is the irreversible loss of funds if a user loses their private key, as there is no central authority like a bank to recover access. This often results from misplaced seed phrases, damaged or lost hardware wallets, or phishing attacks that compromise key security. To mitigate such risks, platforms should prioritize user education, emphasizing the importance of never sharing private keys and securely storing backups, such as using offline metal plates. Encouraging the use of non-custodial wallets like MetaMask or Trust Wallet gives users full control over their keys. Additionally, requiring users to generate and safely store 12- or 24-word seed phrases during wallet setup can help with recovery. For long-term security, implementing inheritance mechanisms—such as a dead man's switch or legally structured recovery plans—can provide a safety net in the event of unforeseen circumstances.

5.2.1.2. Multisig (Multi-Signature) Wallets for Escrow :

Single-key wallets pose significant security risks, as a single compromised key can lead to the complete loss of funds through theft or hacking. A robust alternative is the use of multisignature (multisig) wallets, which require approval from multiple parties—typically 2 out of 3 or 3 out of 5—to authorize a transaction. In the context of car trading, a common multisig setup involves the buyer, seller, and an escrow agent each holding one key. Funds remain locked until at least two of the three participants approve the release, effectively reducing the risk of fraud, such as a seller absconding with the funds before delivering the vehicle. Popular multisig solutions include Gnosis Safe for Ethereum, Bitcoin Core's native multisig features, and Casa, which offers enterprise-level custody services.

5.3. Technical Challenges

5.3.1. Linking with Official Traffic Records Challenges:

Integrating blockchain-based vehicle platforms with government systems presents several challenges due to outdated infrastructure. Many government databases operate on legacy, closed systems that are not designed for API access, and data formats vary widely—ranging from CSV and XML to proprietary schemas—making standardization difficult. Additionally, some registries update ownership records in delayed batches rather than in real time, hindering synchronization. To address these issues, developers can leverage government-approved APIs where available, such as the EU's Vehicle Registration Data (VRD) under the Single Digital Gateway Regulation, certain U.S. state DMV APIs like California's eTitle system, or the UK's DVLA "Share Driving Licence" API (though access is often limited). Where APIs are not accessible, middleware solutions using ETL (Extract, Transform, Load) tools like Apache NiFi can help transform and standardize incoming data. Furthermore, in regions piloting blockchain-based vehicle registries—such as Georgia or the UAE—integration with platforms like Hyperledger Fabric or Ethereum offers a promising path toward modern, decentralized vehicle title management.

5.3.2. On-Chain vs. Off-Chain Data Storage:

On-chain storage is best suited for critical and tamper-resistant data, such as vehicle ownership transfers, lien statuses, and trade agreements. Recording this information directly on the blockchain (e.g., Solana) ensures immutability and provides a transparent, fraud-resistant transaction history. In contrast, off-chain storage should be used for large files and sensitive information. Items like vehicle photos, service records, and maintenance logs are more efficiently stored using decentralized file systems such as IPFS, Arweave, or cloud services like AWS S3. For private or legally sensitive data—such as Know Your Customer (KYC) documents—developers should use encrypted storage solutions or privacy-preserving technologies like zero-knowledge proofs to ensure compliance with data protection standards while maintaining interoperability with blockchain systems.

5.3.3. Risks of Upgradable Programs

While upgradable smart contracts offer flexibility for adapting to new requirements, they also introduce several critical risks. From a security perspective, if the upgrade authority key is compromised, malicious actors could deploy harmful logic, potentially leading to fund theft or data manipulation. Even well-intentioned upgrades can inadvertently introduce breaking changes that disrupt existing data structures or application logic.

On the governance side, upgradability can undermine the core principle of immutability. Government entities or regulatory bodies may be reluctant to trust systems where essential processes—such as vehicle title transfers—can be altered post-deployment. Moreover, contract updates risk falling out of compliance with evolving regulations, especially in areas like Know Your Customer (KYC) protocols.

Data integrity is also at stake. If an upgrade alters the structure or layout of on-chain accounts, previously stored data may become inaccessible or unreadable, breaking historical continuity. This tension between flexibility and trustworthiness underscores the importance of cautious, transparent upgrade mechanisms—preferably governed by multi-signature control or on-chain voting to preserve legitimacy.

5.4. Future Prospects

5.4.1. Cross-Chain Interoperability:

To enable seamless car trading across blockchains such as Solana and Ethereum, the platform should implement cross-chain interoperability using bridges like Wormhole. For example, if a buyer on Ethereum wants to purchase a car listed on Solana, the process involves locking the original car NFT in a Solana escrow PDA, minting a wrapped NFT (wNFT) on Ethereum to represent the asset, and then releasing the funds once the buyer claims the wNFT. This mechanism ensures secure asset transfer across chains, preserves ownership integrity, and expands the marketplace beyond a single network.

5.4.2. Government Reliability & Widespread Adoption:

For mass adoption, governments must standardize vehicle NFTs and automate status updates.

5.4.2.1. Standardizing Car NFTs (National Standards)

Governments can enforce blockchain-based vehicle ownership systems by establishing legal recognition of on-chain titles, treating them as fully equivalent to traditional paper documents. This can be further institutionalized by having departments like the DMV issue official NFTs upon vehicle registration, as seen in initiatives such as Dubai's blockchain-based license program. Additionally, smart contracts can be programmed to automatically calculate and deduct applicable taxes during ownership transfers, ensuring seamless compliance with tax regulations and reducing administrative overhead.

5.4.2.2. Automatic Status Updates (Mileage, Accidents, etc.)

Integrating IoT and oracle systems can significantly enhance the reliability and automation of blockchain-based vehicle platforms. Real-time data, such as mileage, can be streamed directly to Solana PDAs using OBD-II dongles like Automatic or Mojio, while tamper-resistant infrastructure through DePIN networks like Helium or Peaq ensures data integrity. Governments can play a role by running DMV-node oracles that update accident histories on-chain using adapters like Chainlink, while insurance data (similar to Carfax) can be stored on decentralized storage solutions such as Arweave, protected by zero-knowledge proofs for privacy. To encourage user participation, platforms can offer token-based incentives or

discounts for self-reporting maintenance updates, ensuring a more complete and trustworthy vehicle history.

Conclusion

In conclusion, as a result, Web 3.0 has a good future and can solve real-world issues and improve many processes not only in the automotive industry but also in other industries. However, it needs a clear mechanism for interacting with it. In this thesis, a simple platform was implemented as an example to demonstrate how we can solve real-world problems with Web 3.0 and how this can be effective in reducing the time and displacement for users, and how this platform can change the ownership transfer and make it fully autonomous.

Bibliography

[1] Lalav, R. (2022, April 1). *History of the Blockchain, how it all started, and where it's headed?* Bitpowr. https://bitpowr.com/blog/history-of-the-blockchain-how-it-all-started-and-where-it-s-headed

[2] Binance Academy. (2023, May 15). □□□□□ □□□□ □□□□□□□ □□□□□ □□ □□ Binance Academy. https://academy.binance.com/ar/articles/what-is-blockchain-and-how-does-it-work

[3] Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018, October). *Blockchain technology overview* (NIST IR 8202). National Institute of Standards and Technology. https://doi.org/10.6028/nist.ir.8202

[4] Becher, B. (2023, March 23). *What is a consensus mechanism?* Built In. https://builtin.com/blockchain/consensus-mechanism

[5] Ledger. (2024, April 19). *Byzantine fault tolerance in crypto: What is it?* Ledger Academy. https://www.ledger.com/academy/topics/blockchain/byzantine-fault-tolerance-in-crypto-what-is-it

[6] River. (2025). *What is Proof of Work?* https://river.com/learn/what-is-proof-of-work/

[7] Hashcash. (2025). *Hashcash.org*. http://hashcash.org

[8] An, M., Fan, Q., Yu, H., & Zhao, H. (2022). *Blockchain technology research and application: A systematic literature review and future trends*. arXiv. https://arxiv.org/pdf/2306.14802

[9] Digiconomist. (2024). *Bitcoin energy consumption index*. https://digiconomist.net/bitcoin-energy-consumption[]

[10] Ethereum Foundation. (2022, January 26). *Proof-of-stake (PoS)*. https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/

[11] Kraken. (2025). *Proof of stake coins | Top proof of stake tokens by market cap*. https://www.kraken.com/categories/proof-of-stake

[12] Bellaj Badr, R. Horrocks, and Xun (Brian) Wu, *Blockchain by example : a developer's guide to creating decentralized applications using bitcoin, Ethereum, and Hyperledger*. Birmingham: Packt Pub, 2018.

[13] Investopedia. (2019). *Merkle Tree*. https://www.investopedia.com/terms/m/merkle-tree.asp

[14] bitFlyer. (2025). *Coinbase (mining reward)*. https://bitflyer.com/en-us/s/glossary/coinbase

[15] Yakovenko, A. (2017). *Solana: A new architecture for a high performance blockchain v0.8.13*. https://solana.com/solana-whitepaper.pdf

[16] Crypto.com University. (2020). *A deep dive into blockchain scalability*. https://crypto.com/en/university/blockchain-scalability

[17] Equiti. (2024). *Solana vs. Ethereum*. https://www.equiti.com/sc-en/news/crypto-hub/solana-vs-ethereum/

[18] Cryptomus. (2024, August 23). Bitcoin vs Solana: A complete comparison. https://cryptomus.com/ar/blog/bitcoin-vs-solana-a-complete-comparison

[19] "What are digital assets?," @coinbase, 2024. https://www.coinbase.com/learn/crypto-basics/what-are-digital-assets

[20] "Asset Tokenization: Basics, Benefits & Blockchain | Chainlink," chain.link. https://chain.link/education/asset-tokenization

[21] Binance Academy, "Token Standards," Binance Academy, 2025. https://academy.binance.com/en/glossary/token-standards (accessed Jun. 28, 2025).

[22] jdourlens, "Understand the ERC-20 token smart contract," ethereum.org, Apr. 05, 2020. https://ethereum.org/en/developers/tutorials/understand-the-erc-20-token-smart-contract/

[23] "ERC-721 Non-Fungible Token Standard," ethereum.org. https://ethereum.org/en/developers/docs/standards/tokens/erc-721/

[24] W. Radomski, A. Cooke, P. Castonguay, J. Therien, E. Binet, and R. Sandford, "EIP 1155: ERC-1155 Multi Token Standard," Ethereum Improvement Proposals, Jun. 17, 2018. https://eips.ethereum.org/EIPS/eip-1155

[25] "ERC-1155 Multi-Token Standard," ethereum.org. https://ethereum.org/en/developers/docs/standards/tokens/erc-1155/

[26] "Solana Account Model | Solana," Solana.com, 2024. https://solana.com/docs/core/accounts

[27] "Tokens on Solana," Solana.com, 2022. https://solana.com/docs/tokens

[28] Dowling, M. (2022). Is non-fungible token pricing driven by cryptocurrencies? *Finance Research Letters, 44*, 102097. https://doi.org/10.1016/j.frl.2021.102097

[29] ComputerWeekly. (2014). *What is a digital asset?* (Archived on January 8, 2015). https://www.computerweekly.com

[30] Widen. (2022, May 26). *Digital asset management*. https://www.widen.com

[31] Zhang, A., & Gourley, D. (2009). *Creating digital collections*. Oxford: Chandos Publishing.

[32] IDEMIA. (2017, September 19). *Tokenization demystified*. (Archived January 26, 2018). https://www.idemia.com

[33] Ogigau-Neamtiu, F. (2016). Tokenization as a data security technique. *Zeszyty Naukowe AON, 2*(103), 124–135. ISSN 0867-2245.

[34] Rolfe, A. (2015, May). *The fall and rise of tokenization*. Retrieved September 27, 2022.

[35] Xu, X., Pautasso, C., Zhu, L., Lu, Q., & Weber, I. (2018, July 4). A pattern collection for blockchain-based applications. In *Proceedings of the 23rd European Conference on Pattern Languages of Programs* (pp. 1–20). ACM. https://doi.org/10.1145/3282308.3282312

[36] Ozdenizci, B., Ok, K., & Coskun, V. (2016). A tokenization-based communication architecture for HCE-enabled NFC services. *Mobile Information Systems, 2016*, e5046284. https://doi.org/10.1155/2016/5046284

[37] Super Utilisateur. (2025). *Carte d'immatriculation des véhicules*. Site officiel du MICLAT. https://www.interieur.gov.dz/index.php/fr/mes-d%C3%A9marches-administratives/carte-d-immatriculation-des-v%C3%A9hicules

[38] Official Gazette of the People's Democratic Republic of Algeria. (2003). *No. 37*.