

# CS 344 Team Squirtle Blockchain Voucher Platform Project Outline



## Team members:

26259877@sun.ac.za - Yedidia

25526693@sun.ac.za - Caeden

25849611@sun.ac.za - Luke

26429659@sun.ac.za - Izak

26296918@sun.ac.za - David

## Project Specification:

As part of the **impact.com** platform (see <https://impact.com/>) we often connect 3 parties together, who do not necessarily know each other and have no formal relationship, but need to do trusted business with each other.

a) An entity paying for goods (e.g. manufacturer or brand) needs to be certain that only specific goods can be bought by the person receiving the goods. They must be able to guarantee that their money is being spent as intended.

b) An entity providing the goods (e.g. an advertiser) needs to be certain that they will get paid for the goods.

c) An entity receiving goods (e.g. end-user or social influencer) needs to be certain they will receive the goods.

The proposed project will use blockchain (as a public ledger/system of record) to create crypto vouchers that can be issued automatically to provide a 3-way contract between these parties.

The project will involve researching blockchain (and crypto technologies) and providing a platform to request, supply, and verify vouchers. The blockchain also provides a ledger that can be inspected and queried, even for historical contracts.

## **Project Brief:**

### **Objective:**

The project aims to develop a blockchain-based platform that facilitates trusted business transactions between three parties who do not necessarily have formal relationships:

1. **Payer** (e.g., manufacturer or brand)
2. **Provider** (e.g., advertiser)
3. **Receiver** (e.g., end-user or social influencer)

### **Problem Statement:**

In a typical transaction, the payer needs assurance that their funds are used as intended, the provider needs a guarantee of payment, and the receiver needs to trust that they will receive the goods. Traditional methods of ensuring these conditions can be unreliable.

### **Proposed Solution:**

The project will leverage blockchain technology to create crypto vouchers that serve as a 3-way smart contract between these parties. The platform will enable the requesting, supplying, and verifying of these vouchers, ensuring that each party's interests are protected.

### **Scope of work:**

Research on blockchain and crypto technologies.

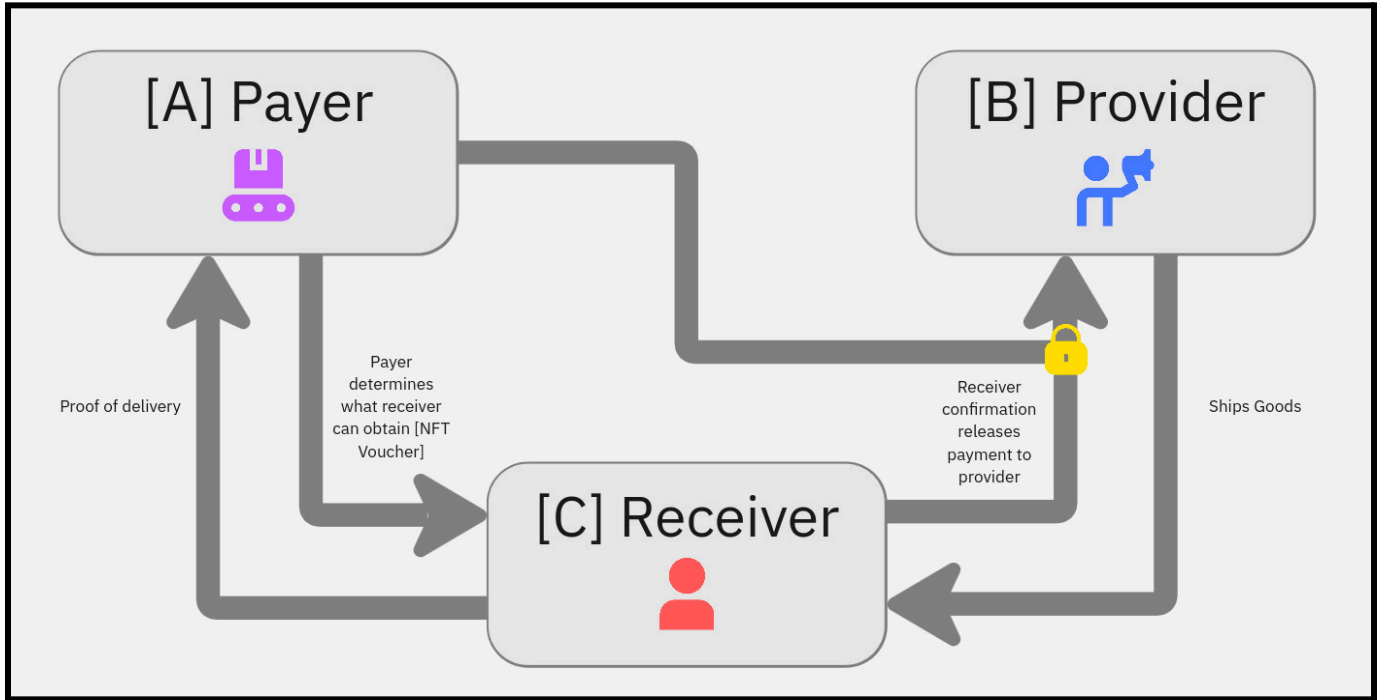
Development of a platform to manage crypto vouchers.

Implementation of features for voucher request, supply, and verification.

This platform will ensure that funds are used as intended, goods are delivered, and payments are made, fostering trust among all parties involved (who do not know each other)..

## Planning:

### Understanding the problem with a diagram:



## Design & Technology Choices:

### 1. Back-end: Solana and Rust

**Solana** is a high-performance blockchain platform known for its fast transaction speeds and low fees, making it ideal for handling the complex transactions required by our 3-way smart contract system.

**Rust** is the primary programming language used for developing on the Solana blockchain. Rust's memory safety and performance characteristics make it a suitable choice for writing secure, efficient smart contracts. These smart contracts will handle the creation, management, and execution of crypto vouchers within our platform.

## 2. Front-end: React, TypeScript, and Solita

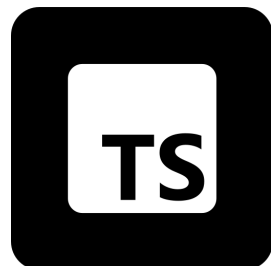
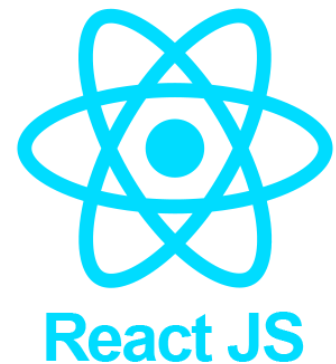
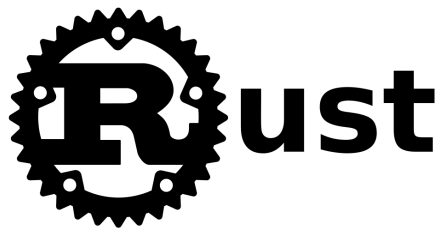
**React** is a widely-used JavaScript library for building user interfaces. Its component-based architecture allows for modular, maintainable code, which is essential for developing a complex frontend.

**TypeScript** is a superset of JavaScript that adds static typing, which helps catch errors early during development and improves the overall reliability of the codebase.

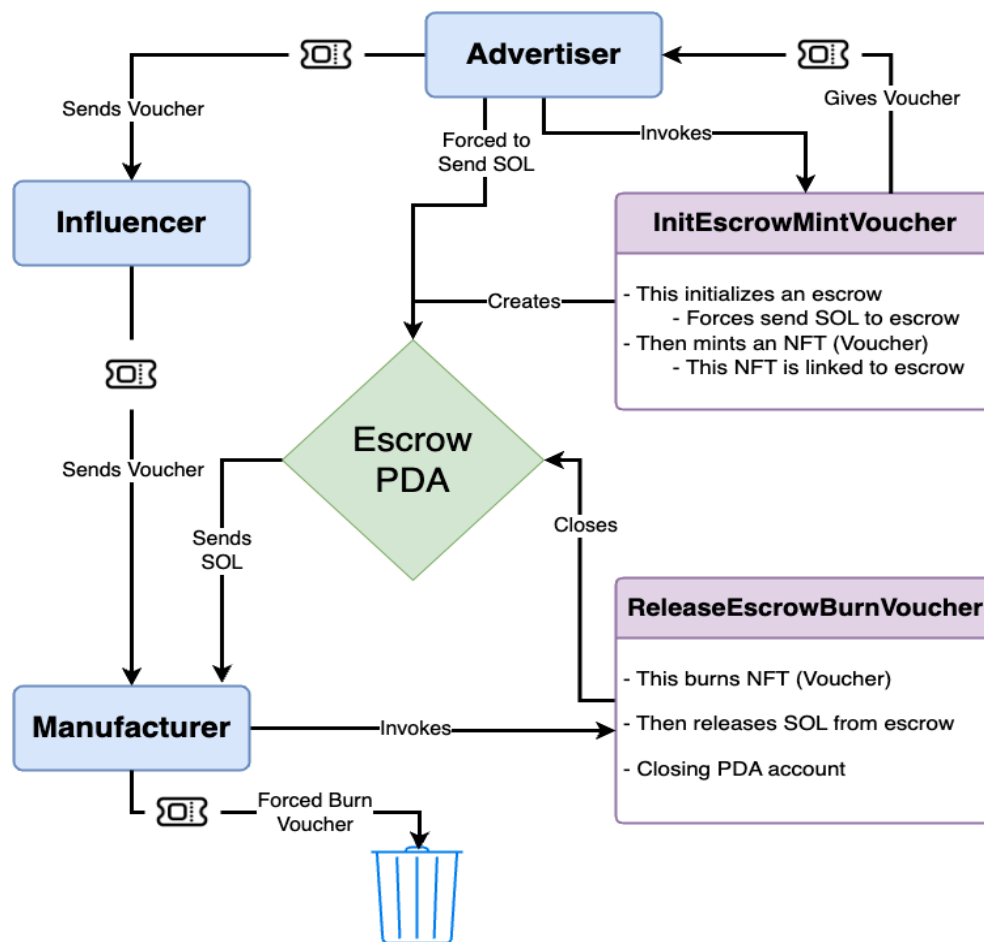
**Solita** is a tool that generates TypeScript bindings from Solana smart contracts (written in Rust). These bindings allow the frontend (React) to interact seamlessly with the blockchain, sending transactions and querying data as needed.

## 3. Development: Git Flow

**Git Flow** is a branching model for Git that defines a strict branching strategy designed around the project release cycle. It allows multiple team members to work simultaneously on different features, bug fixes, and releases without interfering with each other's work, providing structured version control.



## How 3-way smart contracts on the Blockchain will work



### Explanation:

The diagram above illustrates a 3-way interaction between an Advertiser, an Influencer, and a Manufacturer using smart contracts on the Blockchain. The central component of this interaction is the Escrow PDA (Program Derived Address), which manages the flow of funds (SOL) and NFTs (Vouchers).

### How it works:

#### 1. Advertiser:

- Initiates the process by creating a Voucher.
- By creating the Voucher SOL (Solana cryptocurrency) is deposited from their account to the Escrow PDA.
- Sends the voucher to the Influencer.

## 2. Influencer:

- Receives the Voucher from the Advertiser.
- Receives goods from the manufacturer and sends the Voucher to the Manufacturer.

## 3. Manufacturer:

- Receives the Voucher from the Influencer.
- Burns the voucher, which releases the SOL from the escrow PDA which closes the PDA account. All in the same transaction.

## Process Flow:

### 1. Voucher Creation (InitEscrowMintVoucher):

- The Advertiser initiates the smart contract by invoking the `InitEscrowMintVoucher`.
- This instruction deducts SOL from the Advertiser, based on an amount specified by the Advertiser, and sends that SOL to the Escrow PDA, where the funds are securely held.
- Simultaneously, an NFT (Voucher) is minted and linked to the Escrow PDA. This NFT acts as a certificate or proof of the agreement.

### 2. Voucher Exchange:

- The Advertiser sends the Voucher to the Influencer, who then sends it to the Manufacturer, once they receive goods.
- The Manufacturer, after completing their part of the deal (delivering the product or service), sends SOL to the Escrow PDA.

### 3. Voucher Burning (ReleaseEscrowBurnVoucher):

- The Manufacturer invokes the `ReleaseEscrowBurnVoucher` function.
- This burns the NFT (Voucher), signaling the completion of the transaction.
- As a result, the SOL held in the Escrow PDA is released, and the PDA account is closed.

This smart contract mechanism efficiently automates the transaction process, ensuring that payments are only made once all parties have fulfilled their obligations.