5ireChain: Secure Transaction System

This system helps the user send high-value transactions more securely to the receiver.

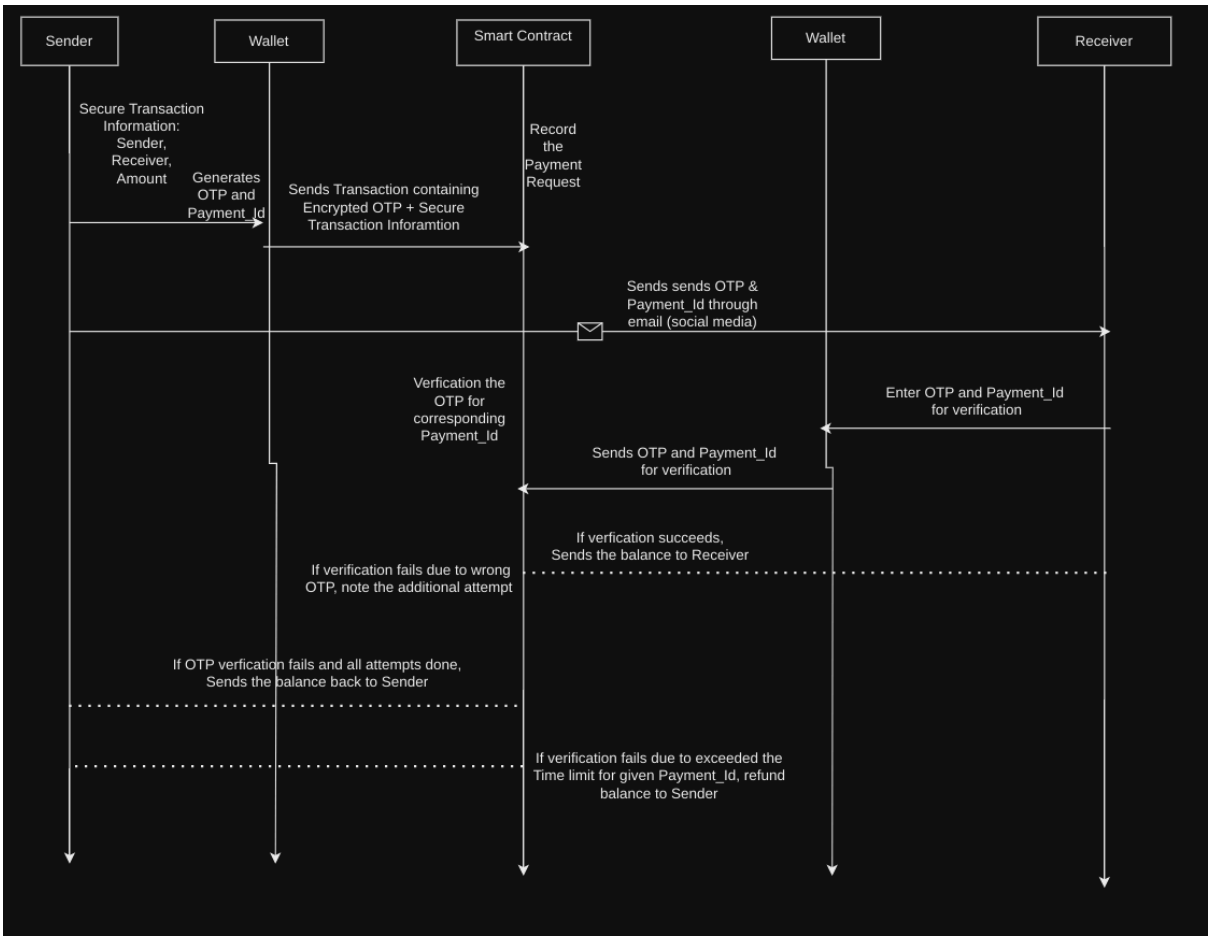
Payment proceeds as usual when the amount in the payment transaction does not exceed the set threshold.

When the amount in the payment transaction exceeds the set threshold,

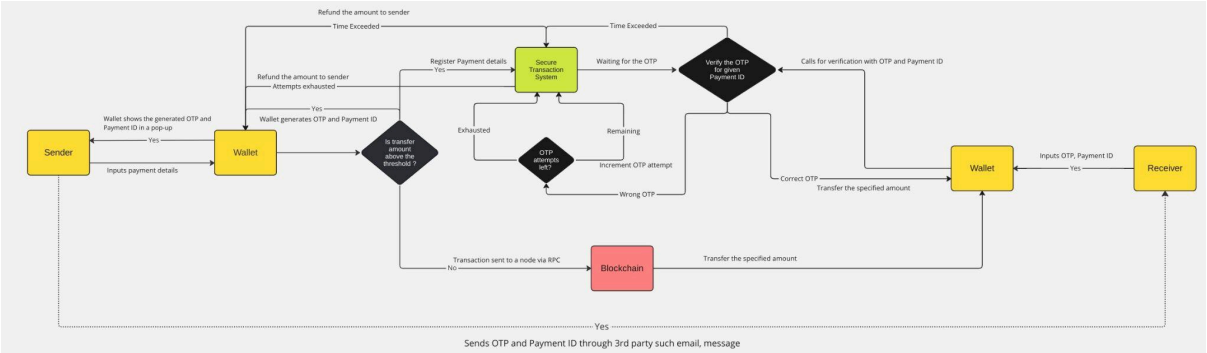
1. The wallet generates an OTP and a PaymentID for the high-value transaction
2. Wallet sends this payment information and required funds to the STS contract.
3. Sender copies the OTP and PaymentID to receiver through social media (say email or any messenger app)
4. Receiver receives the payment only if it has verified the transaction using OTP in STS smart contract within the set time which is by default 1 day.
5. There are a limited number of OTP input attempts available to the Receiver for a given PaymentID.
6. In case of PaymentID expiration, the amount is refunded to the sender by STS contract.

Ultimately, we are securing the high-value token transfer by requiring the Receiver to verify itself on STS contract using the information sent by Sender.

Sequence Diagram:



Block Diagram:



Questions:

- How can I integrate or leverage this module for other chains and crypto wallets?
- What happens when the user key is compromised and the exploiter knows the threshold limit for the user wallet?
- In this security case of a hacked wallet, would a timed limit make sense? If a hacker were to send lots of small transactions, if the cumulative total of those transactions were to reach the threshold limit, then an OTP is generated. Or, the simpler case is to generate an OTP on small transactions (lower than threshold amount) every X number of transactions.

Answers:

- In case of hacked wallet, STS and Wallet could add restrictions:
    - Require OTP from receiver when transaction amount exceeds the set threshold
    - Block the wallet for some hours or days when transactions per minute exceed the set value
    - Block if cumulative total value of txns in 1 hour exceeds the some value
    - Wallet can't send more than 3 high-value STS txn to the same receiver in 1 day
    - User can only change his STS settings in wallet per week or per day