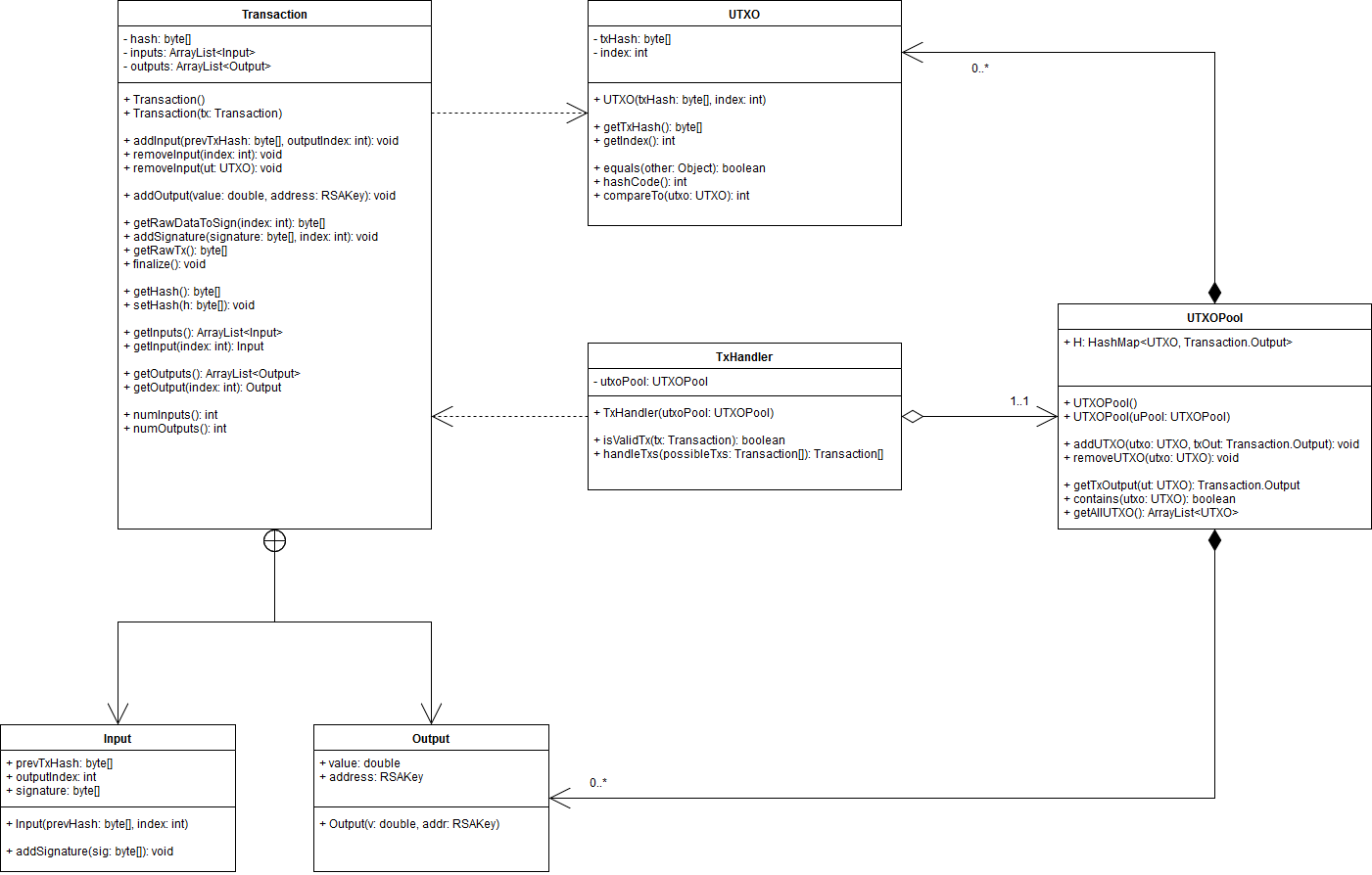
# Security ScroogeCoin opdracht

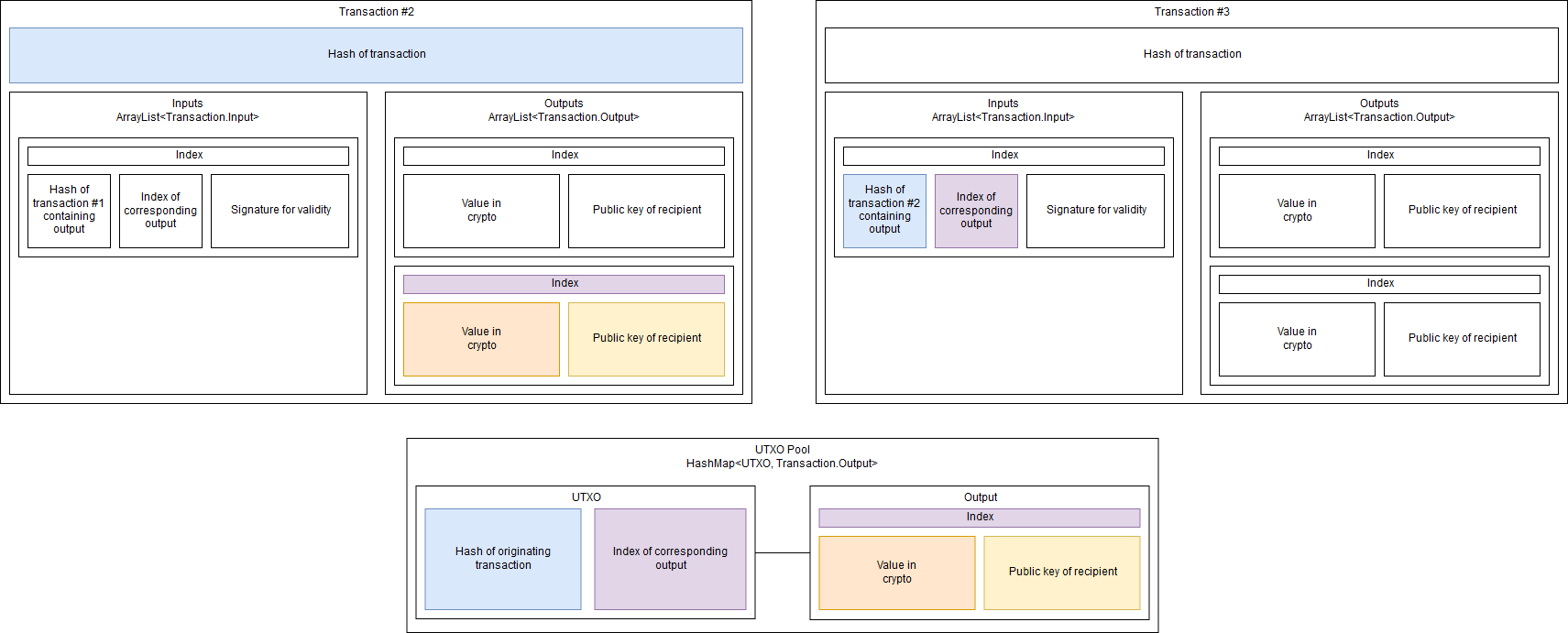
In dit document de uitwerking van de Blockchain opdracht voor Security.

## Opdracht 1



De afkorting UTXO staat voor: **Unspent Transaction Output.** Het is de output van een transacties die nog niet gebruikt is, in principe dus de inhoud van je portemonnee. Wanneer je bijvoorbeeld een briefje van 50, 20 en 5 in je portemonnee hebt zitten, kan dit vertaald worden naar drie UTXO’s. Eén met de waarde 50, één met de waarde 20, en de laatste met de waarde 5 (Daniel, 2018).

## Opdracht 2



De signature is de digest van het originele bericht, wat vervolgens geencrypt is met de private key van de sender.

De signature wordt verkregen door het uitvoeren van de volgende stappen:

1. De message (Transaction.Input) wordt gehasht.
2. Deze digest wordt geëncrypt met de private key van de sender.

Om integriteit en authenticiteit te waarborgen, kan de signature via de volgende stappen geverifieerd worden:

1. De signature kan gedecrypt worden met de public key van de sender. Zo wordt authenticity gewaarborgd. We zijn er zeker van dat de private key de signature heeft gemaakt. Het resultaat van de decryptie is een digest van het originele bericht.
2. Vervolgens kan de ontvanger, het ontvangen bericht opnieuw hashen. Het resultaat kan vergeleken worden met de digest die na decryptie verkregen is. Indien ze gelijk zijn, is het bericht na het ondertekenen niet meer aangepast. Zo is integriteit gewaarborgd.

Het RSA-encryptiealgoritme is gebruikt voor de private/public keys. Verder is SHA-256 gebruikt voor hashing.

SHA-256 wordt ook gebruikt voor het hashen van de transactie.

De input voor de transactie hash is de lijst met inputs, gevolgd met de lijst van outputs, in de vorm van een byte array. Voor de public keys van outputs worden de resultaten van de methodes getExponent() en getModulus() meegenomen als input.

## Opdracht 3

