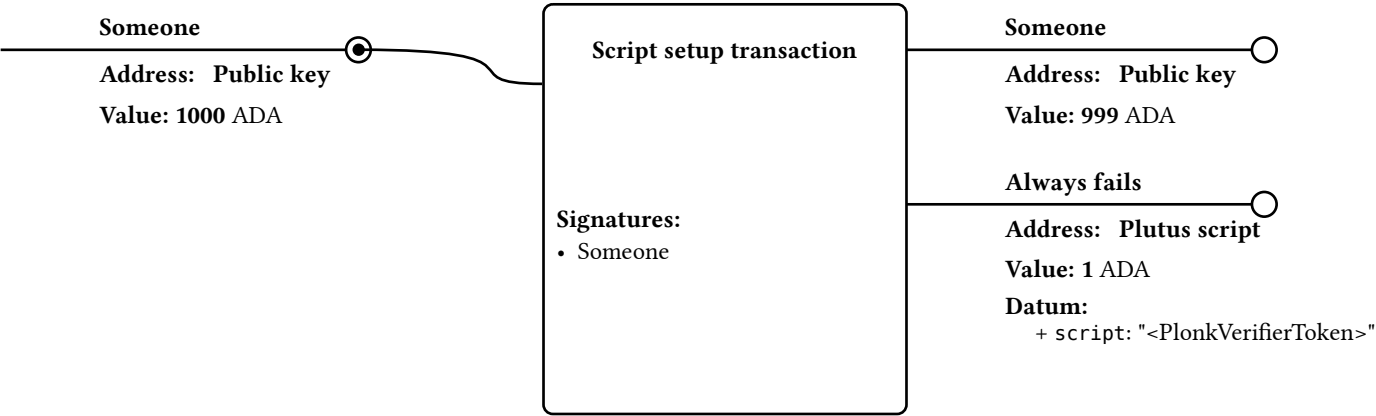


End-to-end test for the PlonkVerifierToken

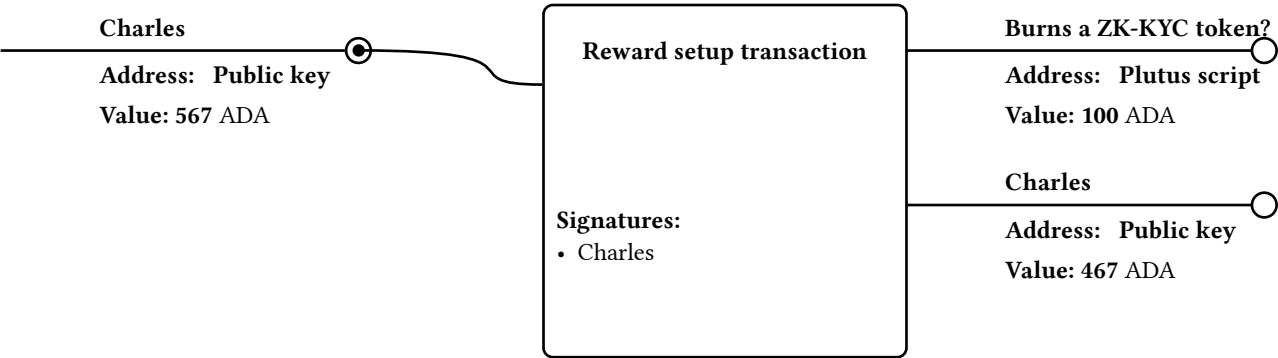
A ZK-KYC scenario: Alice issues a token that represents a cryptographic proof of some statement (KYC info) about Bob and sends the token to him. The minting policy of the token is the Plonk verify algorithm for that statement. Bob can then burn the token in exchange for a reward in ada.

First, we perform a setup transaction that posts the PlonkVerifierToken script on-chain.



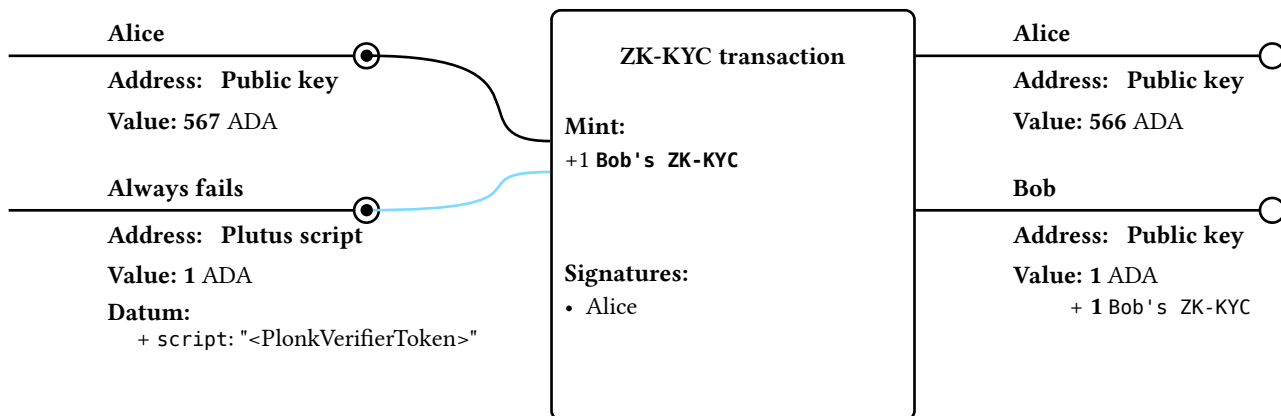
Note: Someone posts the PlonkVerifierToken script on-chain.

In the second transaction, Charles sets up a reward for doing the ZK-KYC process. He sends 100 ada to a Plutus script address. The script unlocks the funds if and only if the KYC token is burned.



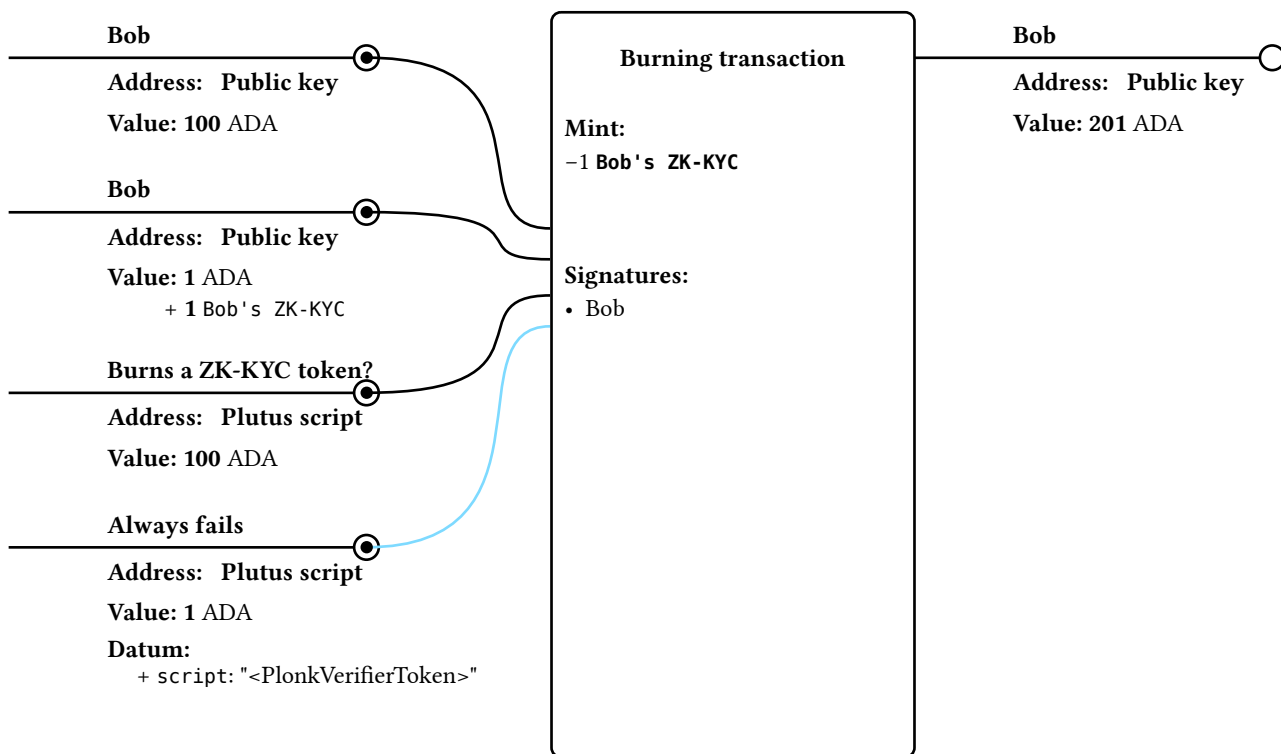
Note: Charles sets up a reward for burning a ZK-KYC token.

Alice can now mint a token that represents a cryptographic proof of some statement about Bob. The minting policy of the token is the Plonk verify algorithm for that statement. In the same transaction, she sends the token to Bob.



Note: Alice mints a ZK-KYC token and sends it to Bob.

Bob can now burn the token and claim the reward.



Note: Bob burns a ZK-KYC token and claims the reward.