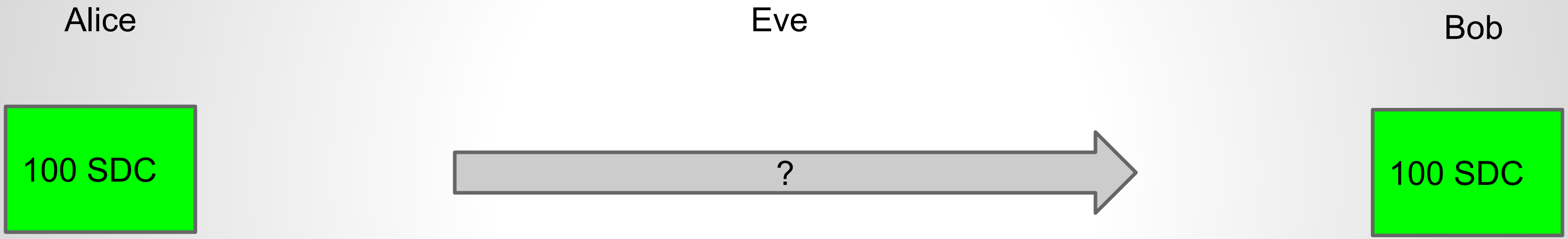
Shadow Transaction Flow

Alice wants to send Bob 100 SDC anonymously without
the onlooker Eve knowing about the transaction.



Alice

Eve

Bob

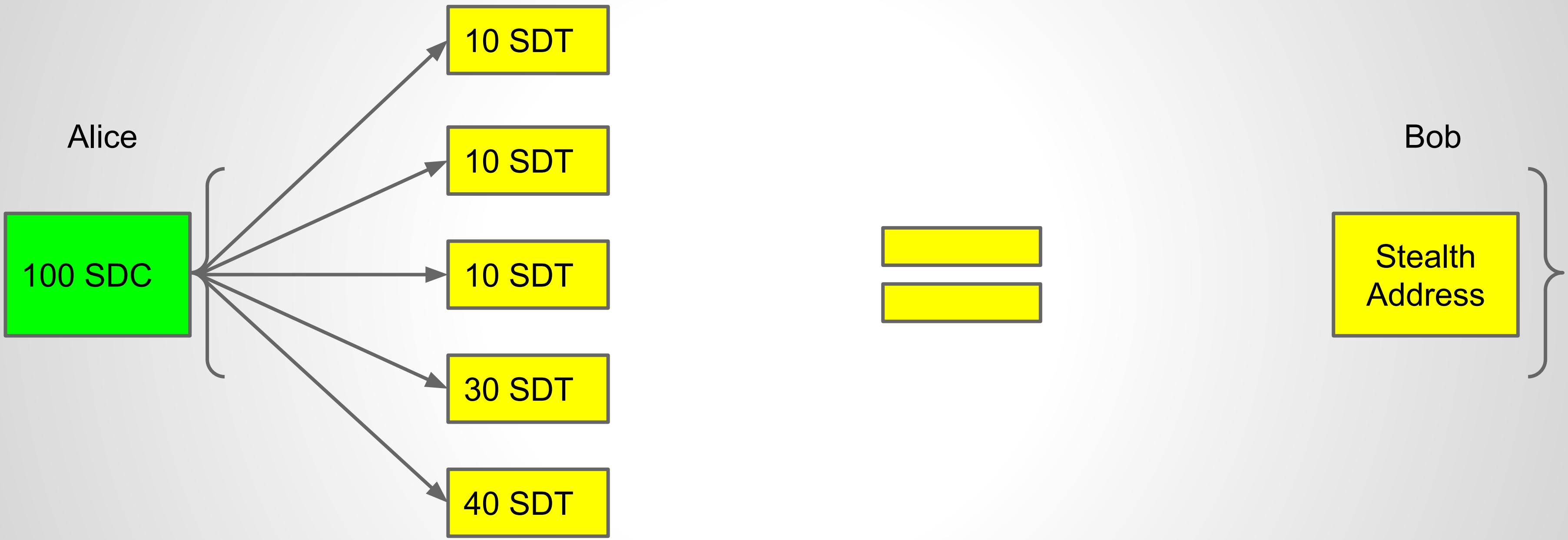
100 SDC

?

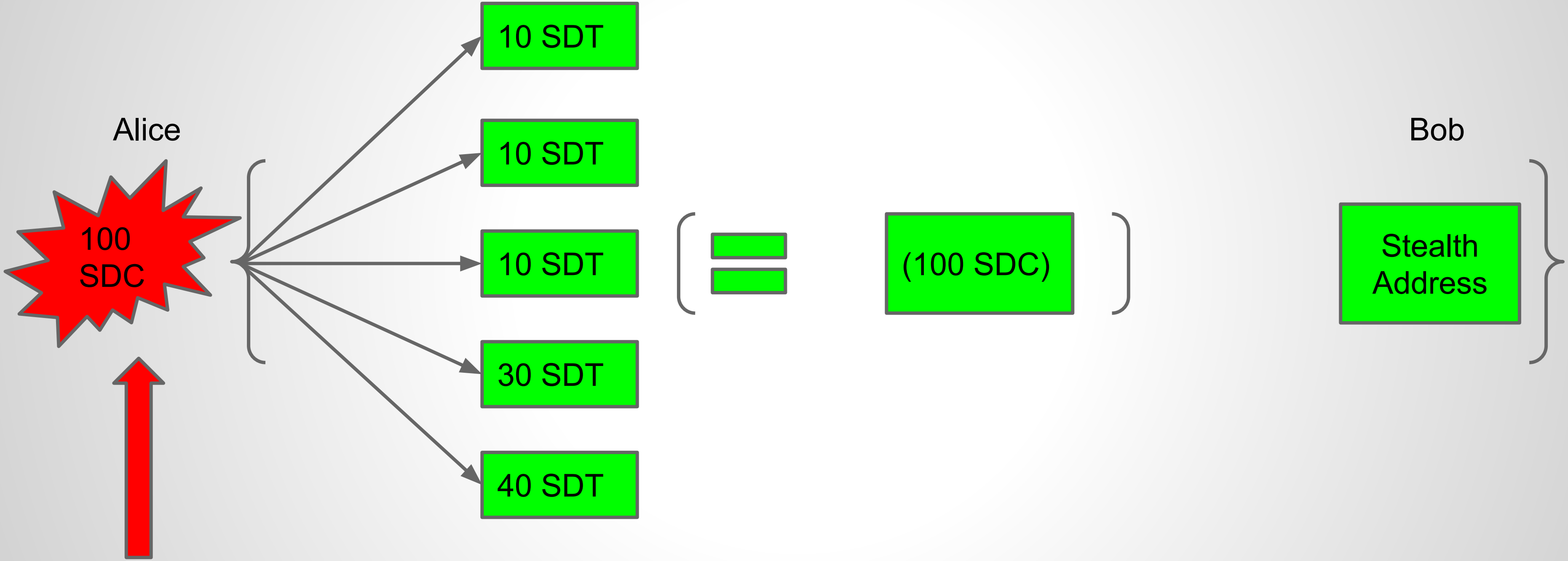
100 SDC

Shadow Transaction Flow

To do this: Alice uses the send ‘SDC-to-Shadow(SDT)’ option to send (the equivalent value) of 100 SDC to Bob’s Dual-key Stealth Address"

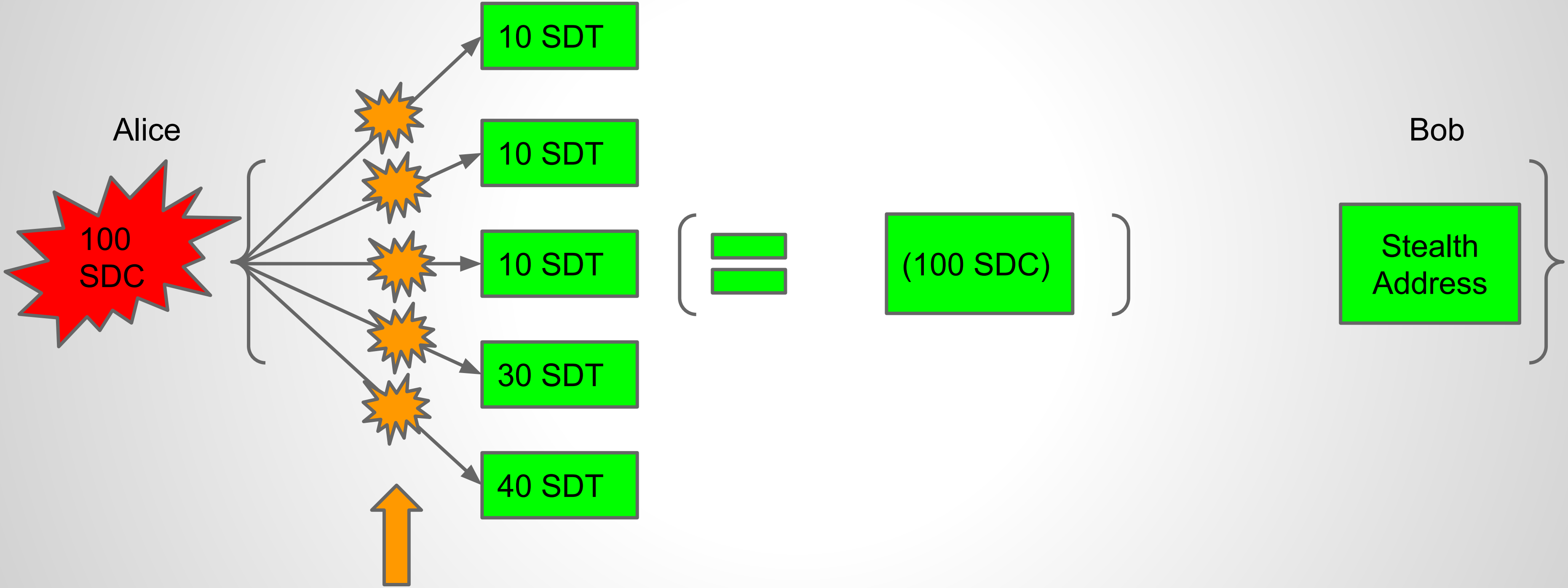


Shadow Transaction Flow



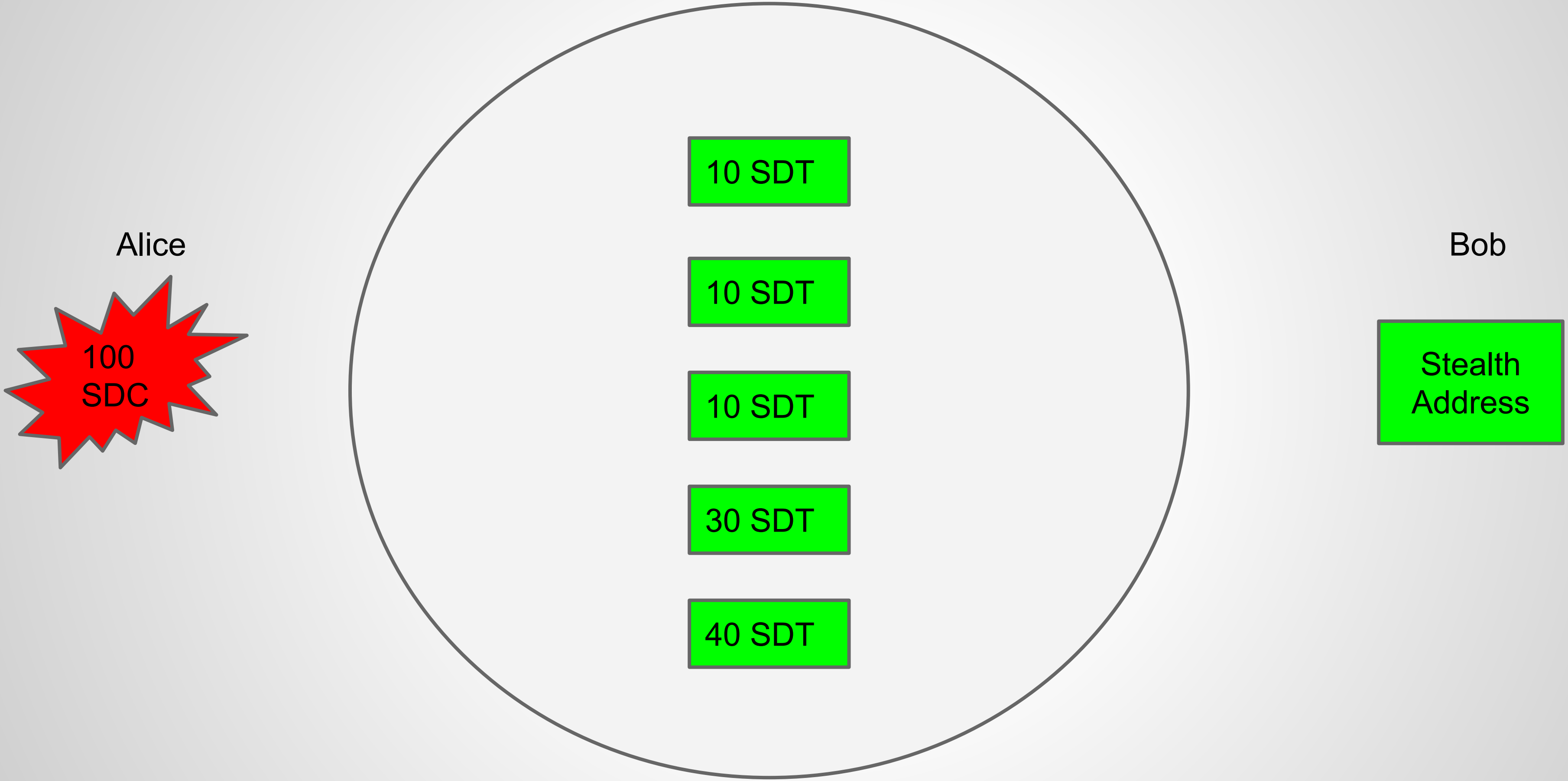
The network destroys the SDC and then mints smaller tokenized denominations of Shadow equal in value to that of the destroyed SDC.

Shadow Transaction Flow



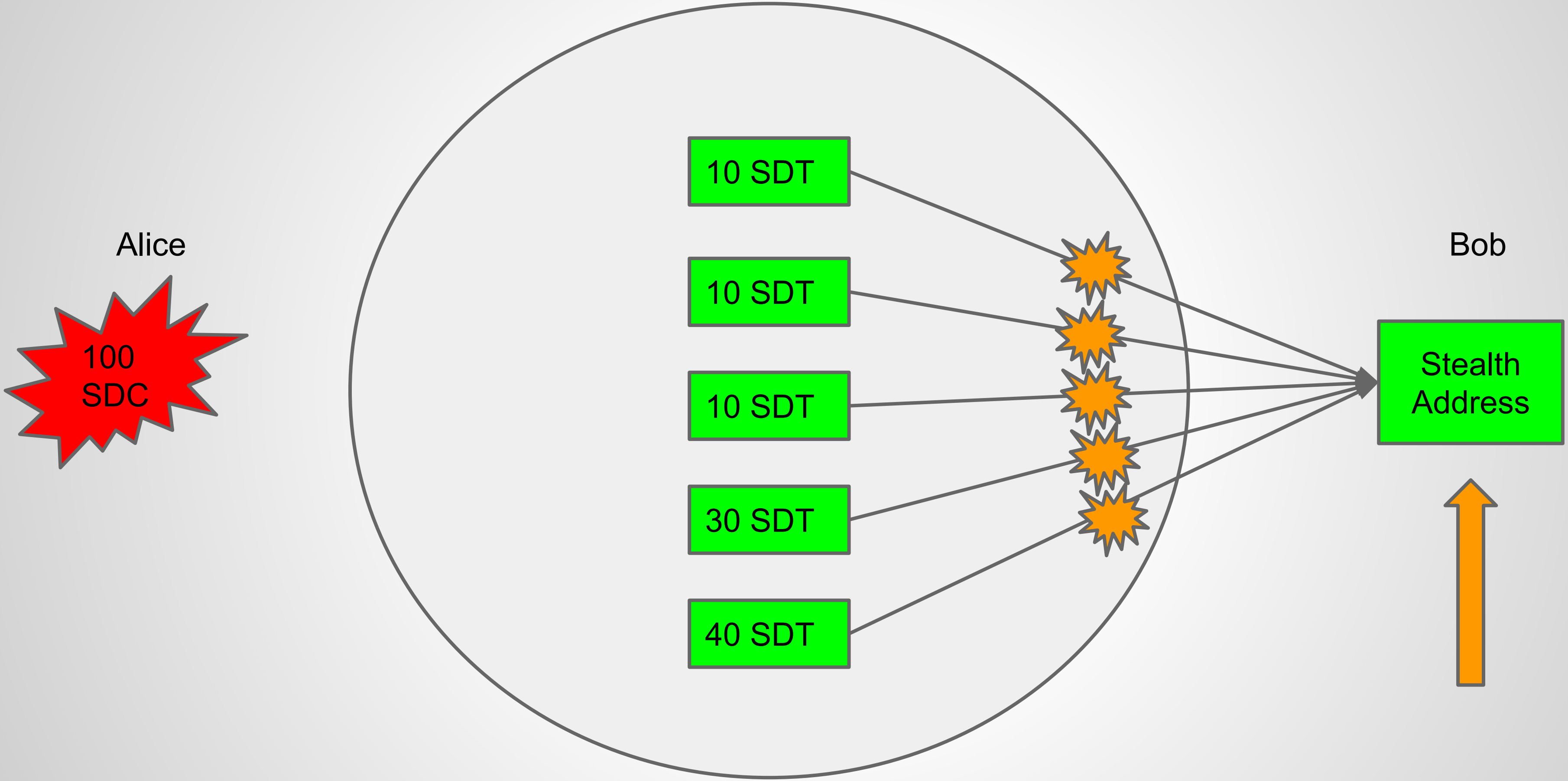
The SDC is minted into Shadow using Dual-Key Stealth Addresses to remove the link between the newly minted Shadow Tokens and the SDC that was destroyed

Shadow Transaction Flow



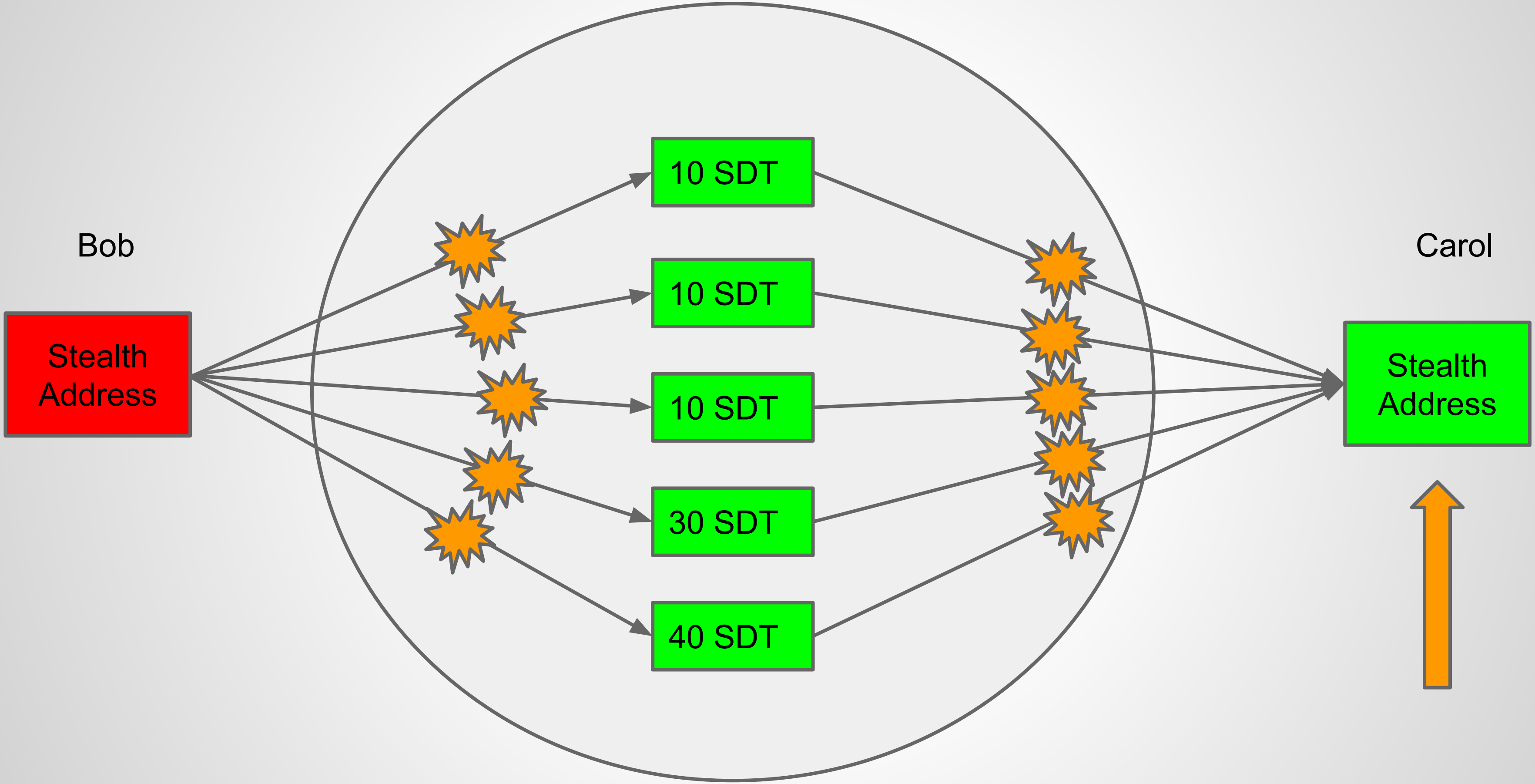
These Shadow Tokens (SDT) make up the members of the ring signature. Non-interactive zero knowledge proofs (NIZKPs) are used when sending Shadow, as each address that a token is sent to, represents the token itself.

Shadow Transaction Flow



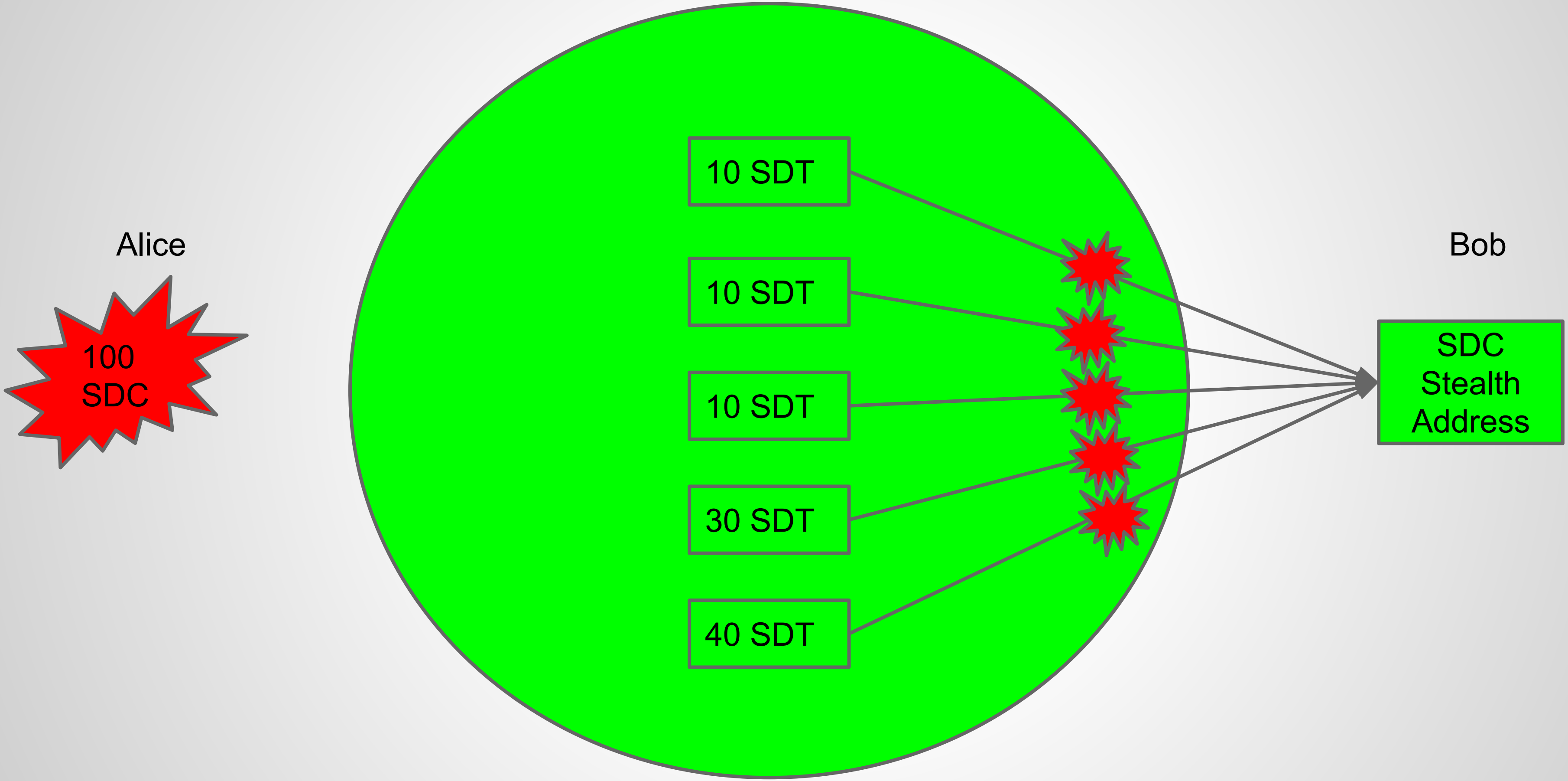
The Shadow tokens (SDT) are sent to dual-key stealth addresses which removes the link between the parties. It is not possible to determine which tokens have been spent, so all tokens remain in the blockchain as spendable outputs available as members of ring signatures for other token spends.

Shadow Transaction Flow



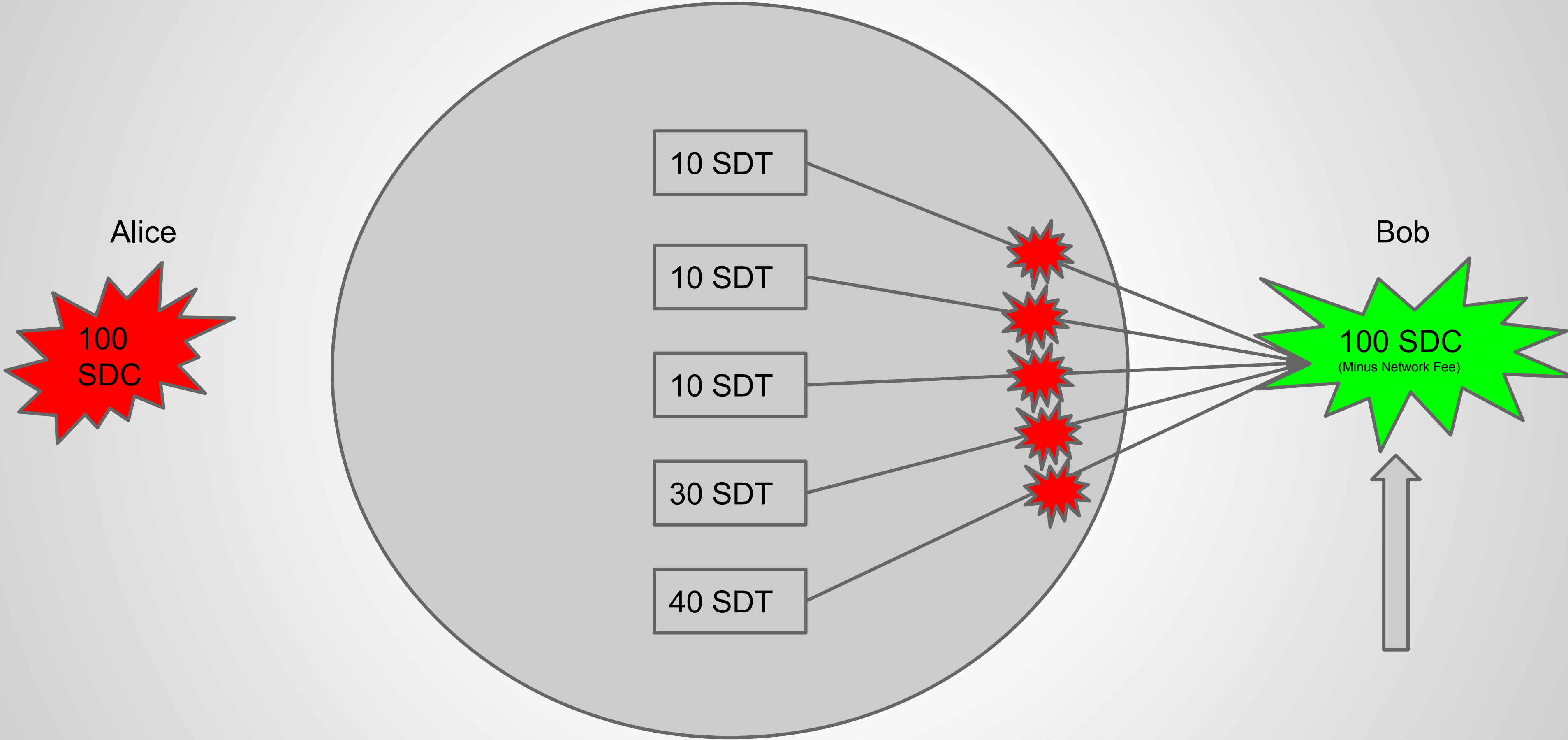
Now that Bob owns the Shadow Tokens, if he chooses, he may Send 100 SDC (worth of SDT) to Carol anonymously. He can do so by sending Shadow to her Stealth Address (Shadow-to-Shadow).

Shadow Transaction Flow



Alternatively, Bob wishes to redeem the Shadow (Shadow-to-SDC) Alice sent him, the network signs the transaction with a ring signature removing traceability

Shadow Transaction Flow



Alice

100 SDC

10 SDT

10 SDT

10 SDT

30 SDT

40 SDT

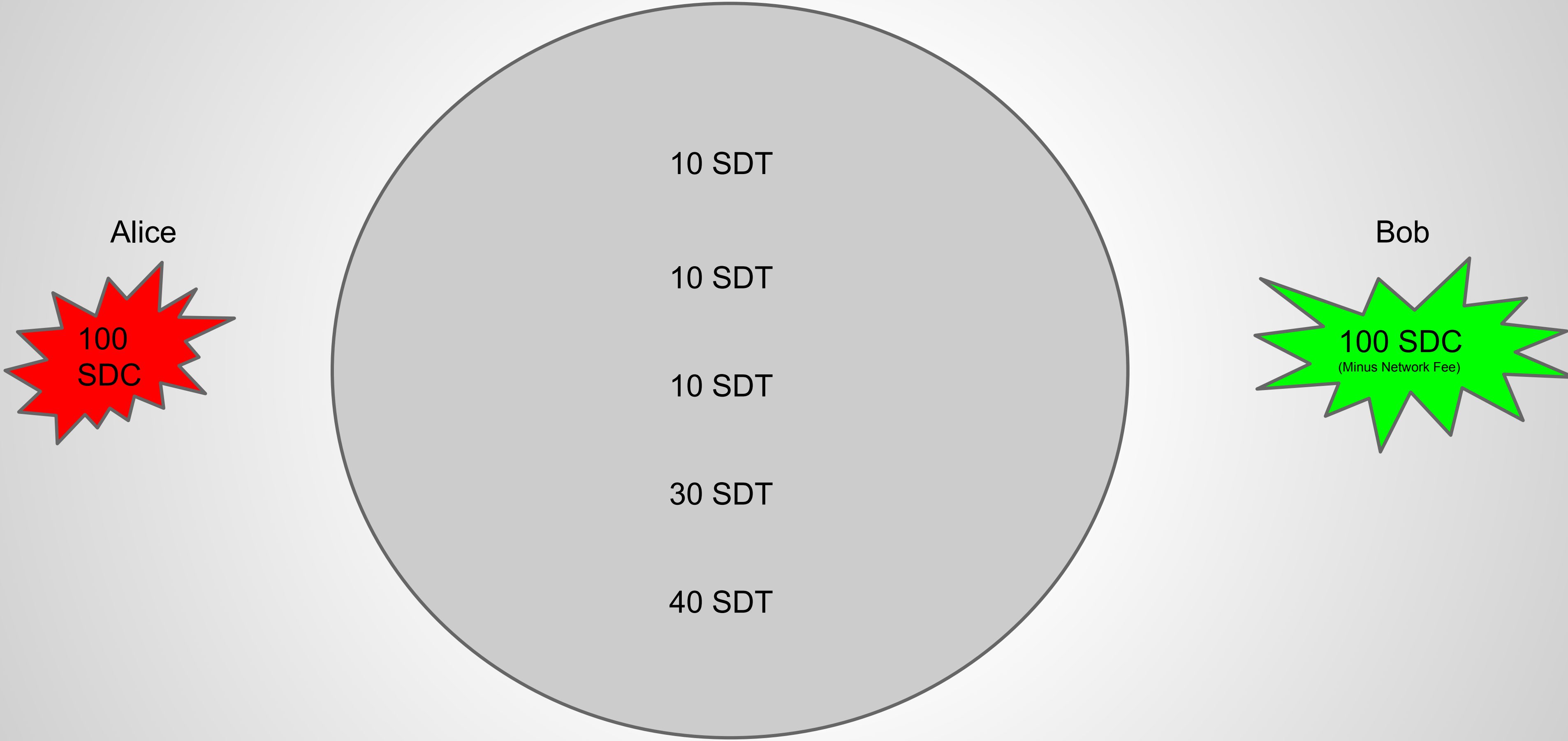
Bob

100 SDC

(Minus Network Fee)

The network mints new SDC equal in value to that of the denominated Shadow tokens (minus the network fee). Shadow tokens take the form of outputs on the ShadowCash chain. Shadow tokens are only spendable by providing a traceable ring signature to prove ownership of the token (Stealth Address). Ownership of the address proves ownership of the tokens. Since we used NIZKP in our traceable ring signature scheme, we don’t reveal any information to anyone.

Shadow Transaction Flow



Alice

100 SDC

10 SDT

10 SDT

10 SDT

30 SDT

40 SDT

Bob

100 SDC

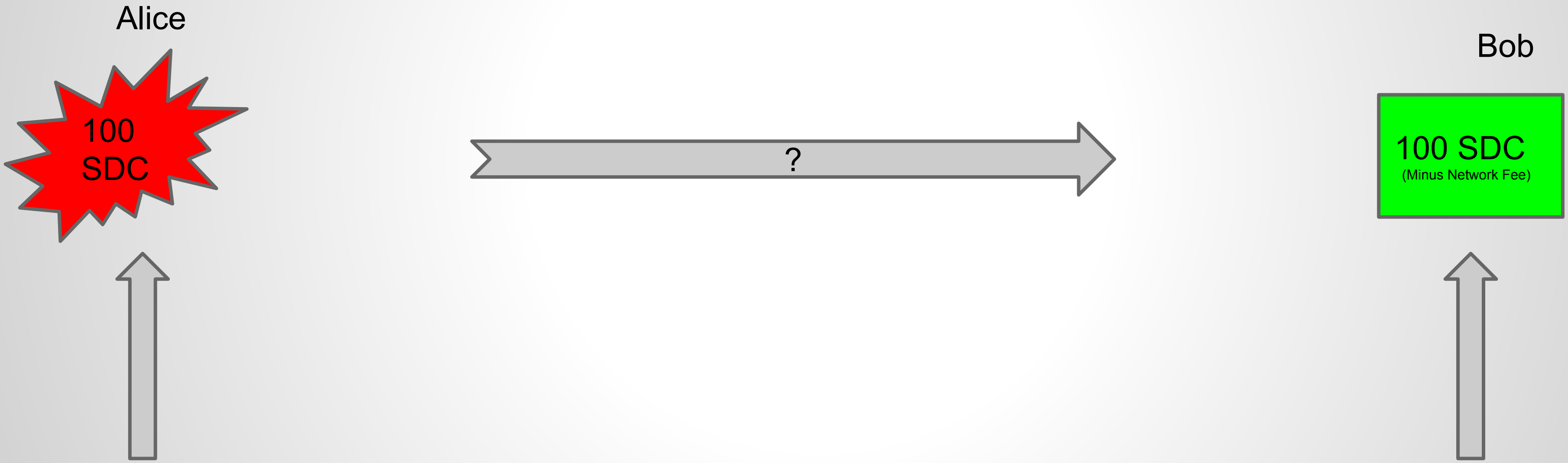
(Minus Network Fee)

The tokens remain in the system increasing the outputs for available ring signatures but cannot used to create any new SDC without a traceable ring. Between 3-200 tokens of each value forms a member of a ring signature, which prevents anyone from knowing which token was spent or who signed the transaction.

Shadow Transaction Flow

Eve

The onlooker can’t establish a link between the two parties and thus has zero knowledge of the transaction



Alice

100 SDC

?

Bob

100 SDC

(Minus Network Fee)

The original SDC was destroyed leaving no connection to the new SDC

The new SDC Bob received has no link or traceable connection to the Shadow Tokens or the original SDC that was destroyed.