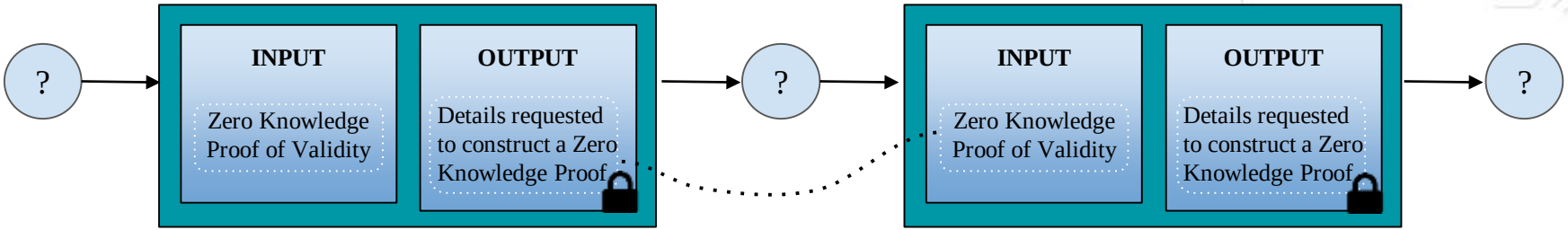
ZSL: Zero-Knowledge Security Layer

zk-SNARKS

- zk-SNARK refers to “**Zero-Knowledge Succinct Non-Interactive Argument of Knowledge.”**
- It allows verification of computational correctness without declaring the knowledge of what was executed among the parties.
- zk-SNARK works on zero-knowledge proof.
- It eventually allows private smart contracts to run on a public blockchain.



TRANSACTION VERIFICATION IN ZCASH

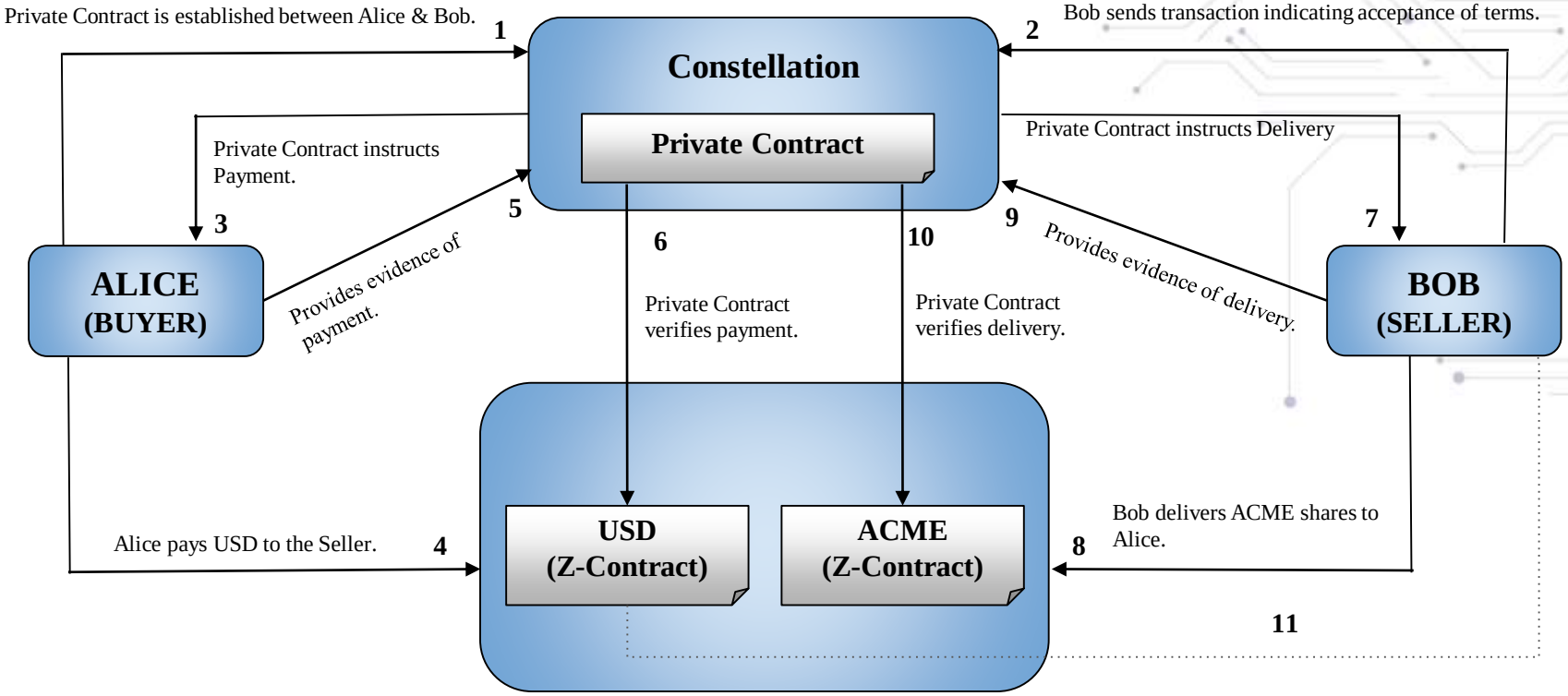
ZSL

- ZSL enables transferring of digital assets without publishing any information of the sender, receiver, and the quantity of assets.
- It ensures the authorization of the sender to transfer the ownership of assets.
- ZSL removes double-spend issue of assets.
- It ensures mass conservation, i.e. transaction input equals its output.

ZSL Components

- **Z-contracts:** A contract that supports the issuance of z-tokens that can be exchanged privately and transparently using ZSL technology.
- **Private Contract:** Trade Parameters like buyer, seller, and the trade lifecycle is defined in the private contract.
- **zk-SNARKS Prover:** The creation of z-transactions requires zk-SNARK prover by the sender who includes proof as part of the transaction that was broadcasted to the network.
- **zk-SNARKS Verifier:** Verifies zk-SNARK proofs attached to the transaction.

ZSL Example



THANK YOU!

Any questions?

You can mail us at

hello@blockchain-council.org