# Assignment 5

### ****Shielding the TX****

*In week 2 you learnt about one of the three use cases of ZK,* ***Privacy****, and how zero-knowledge can be used to shield the identity of both parties in a transaction. This week we will be focusing on privacy within the context of bridges. This is especially useful as we move into a cross-chain era in blockchain, and users require the same level of anonymity when bridging their tokens across different chains*

1. *You have been asked to present a mechanism that will allow a user to bridge 100,000 UST tokens privately and securely from Ethereum to Harmony. Draft a write-up explaining the protocol to be built to cater for this need, highlighting the challenges to be faced and potential resolution to them.*

**[ANSWER]**

1. *In February 2022, a hack on a popular crypto bridge led to the second biggest crypto heist where $320m was lost. Following the technical details behind the hack, it is very clear that bridge smart contracts need to be airtight to prevent scrupulous individuals from taking advantage of them. Briefly explain key mechanisms you will put in place in your interoperable private bridge (specifically the withdrawal methods) to prevent a similar attack (Double withdrawal and fake withdrawal).*

**[ANSWER]**

1. ***[Bonus]*** *Design a smart contract to be deployed on both blockchain to take care of the user’s request and circuits to take care of the privacy*

**[ANSWER]**

### Aztec

[*AZTEC protocol*](https://github.com/AztecProtocol/AZTEC/blob/a383f86b094eda9c361a45c7aade81d28fa99f46/AZTEC.pdf) *utilizes a set of zero-knowledge proofs to define a confidential transaction protocol, to shield both native assets and assets that conform with certain standards (e.g. ERC20) on a Turing-complete general-purpose computation.*

1. *Briefly explain the concept of AZTEC Note and how the notes are used to privately represent various assets on a blockchain. There are various proofs utilized by the AZTEC protocol including range proofs, swap proofs, dividend proofs and join-split proofs. Highlight the features of these proofs and the roles they play in creating confidential transactions on the blockchain*

**[ANSWER]**

1. **[Infrastructure Track Only]** Using the [loan application](https://github.com/AztecProtocol/loan-dapp-starter-kit) as a reference point, briefly explain how AZTEC can be used to create a private loan application on the blockchain highlighting the benefits and challenges. In the Loan Application, explain the Loan.sol and LoanDapp.sol file (comment inline)

**[ANSWER]**

### Webb

*Webb protocol is tornado cash with a bridge built on top of it.* [*EVM code*](https://github.com/webb-tools/protocol-solidity)***,*** [*relayer code*](https://github.com/webb-tools/relayer)*,* [*substrate code*](https://github.com/webb-tools/protocol-substrate)*(in development). Webb is not live yet, it’s only on testnet. Code is not yet complete so be aware of that while reading it.*

1. What is the difference between commitments made to the mixer, Anchor and VAnchor contracts? Can you think of a new commitment structure that could allow for a new feature? (eg: depositing one token and withdrawing another?) if so, what would the commitment look like?

**[ANSWER]**

1. *Describe how the UTXO scheme works on the VAnchor contract.*

**[ANSWER]**

1. ***[Infrastructure Track Only] Explain how the relayer works for*** [***the deposit part of the mixer protocol***](https://github.com/webb-tools/relayer/blob/main/src/events_watcher/tornado_leaves_watcher.rs#L82)

**[ANSWER]**

1. ***[Bonus]*** *Write a program using ethers-rs to interact with the dark-forest smart contract you created for assignment 3.*

**[ANSWER]**

### Thinking In ZK

1. *If you have a chance to meet with the people who built the above protocols what questions would you ask them?*

**[ANSWER]**