# Assignment 2

### *Question 1: Privacy & ZK VMs*

1. ***Explain in brief, how does the existing blockchain state transition to a new state? What is the advantage of using verification over re-execution?***  
     
   **[Answer]** To make a change of state, one submits some input data as a transaction to the blockchain network. This transaction will be verified by a group of miners (PoW) or validators (PoS) to determine its validity. They do so by re-executing the State Transition Function using the user input data and comparing the results with each other. If most of them reach an agreement, the chain state will be altered, and the transaction will be permanently stored in the blockchain.   
     
   The advantage of using verification over re-execution:  
     
   1) *Privacy*. Users don’t need to submit their input data to the public network for nodes to verify the validity of their transaction. As a result, both the input data and the STF is not exposed to the public.  
     
   2) *Scalability*. The throughput of a blockchain network is notoriously slow. This is in part due to the computation overhead caused by the re-execution of each transaction in each node. If the time it takes to verify each transaction becomes shorter, the overall processing capability of the network will improve tremendously.  
     
   3) *Computation Restriction.* If one tries to perform complex computation in a smart contract on chain, the gas fee will explode. Not to mention to re-execute this computation on each node. This limits the functionality of a smart contract in a blockchain. For many real-world use cases and more complicated computations, verification can circumvent this limitation.  
     
   4) Storage Usage. As re-execution is the only way to restore the chain state, the transaction history of a blockchain must be stored in full across all the nodes and crease exponentially. Verification does not need to store all these histories and thus is more storage efficient.
2. ***Explain in brief what is a ZK VM (virtual machine) and how it works?***

**[Answer]** A ZK VM is a circuit (a representation of a program) that executes bytecode. It allows a prover to show that, given a set of inputs, as well as some bytecode, they have correctly executed the program code on said inputs.

* 1. ***Give examples of certain projects building Zk VMs (at-least 2-3 projects). Describe in brief, key differences in their VMs.*[Answer]**  
     1) *zkEVM*: a technology powers zkSync 2.0, is a virtual machine that executes solidity smart contracts in a way that is compatible with zero-knowledge-proof computation using ZK-SNARK.  
       
     2) *Distaff*: a zero-knowledge virtual machine running a proprietary program syntax. For any program executed on Distaff VM, a STARK-based proof of execution is automatically generated. zCloak is based on this VM.  
      3) *Cairo*: A Turing-complete language and VM making it possible for blockchain developers to harness the power of STARKs. It runs on StarkNet which is a permissionless decentralized ZK-Rollup operating as an L2 network over Ethereum, where any dApp can achieve unlimited scale for its computation, without compromising Ethereum’s composability and security.

4) *snarkvm:* based on ZK-SNARK proof technology and executes Leo Programming Language and running on Aleo blockchain. Aleo offers very good developer tool as Aleo Studio.

* 1. ***[Bonus] What are the advantages and disadvantages of some of the existing Zk VMs?***

**[Answer]**

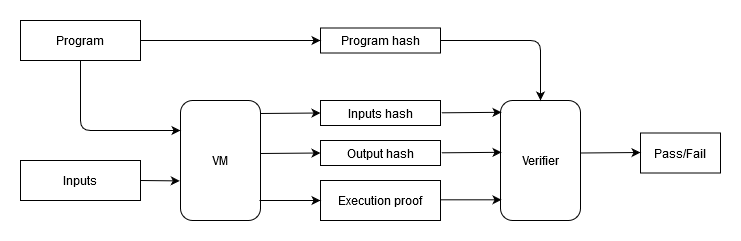
Advantage:

1. The program, the inputs, and the outputs are fully private (they are never revealed to the verifier).
2. A single verifier can verify any program executed on the VM (e.g. a verifier can be a single on-chain contract).
3. A ZK VM abstracts away some tricky aspects of writing circuits. While developers should still understand the underlying system on which their code will run for security reasons, it is theoretically easier to write code for a VM than wiring a circuit by hand.
4. Since the structure of the STARK is the same for all programs, batching of proofs using another STARK (or a SNARK) should be much easier to accomplish.

Disadvantage:

* + - 1. Vendor lock-in, the current selection of ZK VMs available is small, and some ZK VM authors have indicated that they may exercise a greater degree of control over their platforms than is usually seen in fully open-source projects.
      2. Could be slower compared to dedicate circuit application, ZK VM could have poor performance if the circuit is small.
  1. ***[Bonus] Explain in detail one of the Zk VM architectures using diagrams.***

**[Answer]**



In the above:

1. The VM does the following:  
   a. Takes 2 inputs: a program and a set of inputs for the program,  
   b. Executes the program with the given set of inputs,  
   c. Outputs hash of the inputs, hash of the outputs generated by the program, and a STARK proof attesting to the correct execution of the program.
2. The verifier does the following:  
   a. Takes the hash of the program, hash of the inputs, and hash of the outputs, and uses them to verify the STARK proof.

### *Question 2. Semaphore*

1. ***What is Semaphore? Explain in brief how it works? What applications can be developed using Semaphore (mention 3-4)?***  
     
   **[Answer]** Semaphore is a zero-knowledge gadget which allows Ethereum users to prove their membership of a set without revealing their original identity. At the same time, it allows users to signal their endorsement of an arbitrary string and provides a simple built-in mechanism to prevent double-signalling or double-spending. It is designed to be a simple and generic privacy layer for Ethereum DApps.   
     
   This gadget comprises of smart contracts and zero-knowledge components which work in tandem. The Semaphore smart contract handles state, permissions, and proof verification onchain. The zero-knowledge components work offchain to allow users to generate proofs, which allow the smart contract to update its state if these proofs are valid.  
     
   Use cases include private voting, whistleblowing, mixers (Tornado Cash), and anonymous authentication.
2. ***Clone the semaphore repo (***[***3bce72f***](https://github.com/appliedzkp/semaphore/commit/3bce72febeba48454cb618a1f690045c04809900)***).***
   1. ***Run the tests and add a screenshot of all the test passing.*[Answer]  
      *Text

      Description automatically generated***
   2. ***Explain code in the sempahore.circom file (including public, private inputs).***

**[Answer]** see <https://github.com/geesimon/zku/blob/main/week2/semaphore.circom>

* 1. ***[Bonus] Create a frontend for the current semaphore [version](https://github.com/appliedzkp/semaphore/commit/3bce72febeba48454cb618a1f690045c04809900" \t "_blank). You can use [this](https://github.com/weijiekoh/semaphore-ui" \t "_blank) as reference.*[Answer]**

1. Use [Elefria](https://www.elefria.com/" \t "_blank) protocol on the [Harmony Testnet](https://testnet.elefria.com/" \t "_blank), try to generate a ZK identity and authenticate yourself as a user.  
    **[ScreenShots]**

.Graphical user interface, application

Description automatically generatedGraphical user interface, text, application

Description automatically generated

* 1. What potential challenges are there to overcome in such an authentication system?  
       
     **[Answer]**From the end user experience perspective,
     1. Such authentication seems quite slow compared with centralized authentication process (a.k.a, Facebook, Google). This could be due to the fact user needs to generate witness and proof each time when login.
     2. Since the secret is stored in browser’s local storage, user must authenticate twice (one to decrypt the secret, one to login to MetaMask), which is quite redundant.
     3. Every time, user registers or logins, MetaMask will popup asking for fee (pay gas), I feel this could be a deal breaker for user adoption since no app/web applications charge this kind of fee today. We probably should transfer such gas consumption to the web3 developer to relief user concerns.

From Web3 developer perspective,

* + - * When authentication is ZK, web3 developers need a new way to customize user experience base on their personal data and the solution is not quite there yet. Think of how to build a Amazon product recommendation in the ZK world.
      * In case, user cleaned the browser, he probably cleaned all registered and personal tracking info. We need a better way to store user personal info (in IPFS?) to avoid such disaster.
      * Since web3 app doesn’t know which account is active, it creates big challenge to business to do customer based BI analysis and CRM in order to improve customer satisfaction.
  1. [Bonus] What potential improvements can one make to simplify the Elefria authentication protocol?  
       
     **[Answer]** I think we could combine Connect Wallet, Register and Login processes in one process (Login), when user click on Login,
     1. Check whether wallet is connected, if not, connect the wallet.
     2. Check whether the user has already registered, if not, start the registration process.
     3. Start the login process.
        + Also in this process, its unnecessary to ask user to enter password everytime in order to decrypt the secret. Instead, we could make a feature like, “login automatically in 15 days” to futhur simplify the login process.