# Assignment 4

### ****Which stream do you choose (answer with A or B)?****

**[ANSWER]** A

### ****Scaling the future****

*In the blockchain there is a well-known scalability trilemma. We can’t have decentralized, secure, and scalable L1 blockchain. Many blockchains tend to be secure and decentralized, but they lack scalability.*

1. *Based on the above, a few solutions have been proposed to solve this trilemma. Briefly describe the different scalability solutions and write pros and cons of each approach. What was the biggest problem with the Plasma approach?*

**[ANSWER]**

* **STATE CHANNELS**: State channels allow participants to transact x number of times off-chain while only submitting two on-chain transactions to the Ethereum network. This allows for extremely high transaction throughput.
  + Pros:
    - Instant withdrawal/settling on mainnet (if both parties to a channel cooperate).
    - Extremely high throughput is possible.
    - Lowest cost per transaction - good for streaming micropayments.
  + Cons:
    - Time and cost to set up and settle a channel - not so good for occasional one-off transactions between arbitrary users.
    - Need to periodically watch the network (liveness requirement) or delegate this responsibility to someone else to ensure the security of your funds.
    - Have to lockup funds in open payment channels.
    - Don't support open participation.
* **SIDECHAINS**: A sidechain is a separate blockchain which runs in parallel to Ethereum mainnet and operates independently. It has its own consensus algorithm (e.g. proof-of-authority, Delegated proof-of-stake, Byzantine fault tolerance). It is connected to mainnet by a two-way bridge.
  + Pros:
    - Established technology.
    - Supports general computation, EVM compatibility.
  + Cons:
    - Less decentralized.
    - Uses a separate consensus mechanism. Not secured by layer 1 (so technically it’s not layer 2).
    - A quorum of sidechain validators can commit fraud.
* **PLASMA:** A plasma chain is a separate blockchain that is anchored to the main Ethereum chain and uses fraud proofs (like optimistic rollups) to arbitrate disputes. These chains are sometimes referred to as "child" chains as they are essentially smaller copies of the Ethereum mainnet. Merkle trees enable creation of a limitless stack of these chains that can work to offload bandwidth from the parent chains (including mainnet). These derive their security through fraud proofs, and each child chain has its own mechanism for block validation.
  + Pros:
    - High throughput, low cost per transaction.
    - Good for transactions between arbitrary users (no overhead per user pair if both are established on the plasma chain).
  + Cons:
    - Does not support general computation. Only basic token transfers, swaps, and a few other transaction types are supported via predicate logic.
    - Need to periodically watch the network (liveness requirement) or delegate this responsibility to someone else to ensure the security of your funds.
    - Relies on one or more operators to store data and serve it upon request.
    - Withdrawals are delayed by several days to allow for challenges. For fungible assets this can be mitigated by liquidity providers, but there is an associated capital cost.
* **VALIDIUM:** Uses validity proofs like ZK-rollups but data is not stored on the main layer 1 Ethereum chain. This can lead to 10k transactions per second per validium chain and multiple chains can be run in parallel.
  + - Pros:
      * No withdrawal delay (no latency to on-chain/cross-chain tx); consequent greater capital efficiency.
      * Not vulnerable to certain economic attacks faced by fraud-proof based systems in high-value applications.
    - Cons:
      * Limited support for general computation/smart contracts; specialized languages required.
      * High computational power required to generate ZK proofs; not cost effective for low throughput applications.
      * Slower subjective finality time (10-30 min to generate a ZK proof) (but faster to full finality because there is no dispute time delay).
      * Generating a proof requires off-chain data to be available at all times.
  + **OPTIMISTIC ROLLUPS:** Optimistic rollups sit in parallel to the main Ethereum chain on layer 2. They can offer improvements in scalability because they don't do any computation by default. Instead, after a transaction, they propose the new state to mainnet. With Optimistic rollups, transactions are written to the main Ethereum chain as calldata, optimizing them further by reducing the gas cost.
    - Pros:
      * Anything you can do on Ethereum layer 1, you can do with Optimistic rollups as it's EVM and Solidity compatible.
      * All transaction data is stored on the layer 1 chain, meaning it's secure and decentralized.
    - Cons:
      * Long wait times for on-chain transaction due to potential fraud challenges.
      * An operator can influence transaction ordering.
  + **ZERO-KNOWLEDGE ROLLUPS:** Zero-knowledge rollups (ZK-rollups) bundle (or "roll-up") hundreds of transfers off-chain and generate a cryptographic proof. These proofs can come in the form of SNARKs or STARKs and get posted to layer 1.

The ZK-rollup smart contract maintains the state of all transfers on layer 2, and this state can only be updated with a validity proof. This means that ZK-rollups only need the validity proof instead of all transaction data. With a ZK-rollup, validating a block is quicker and cheaper because less data is included.

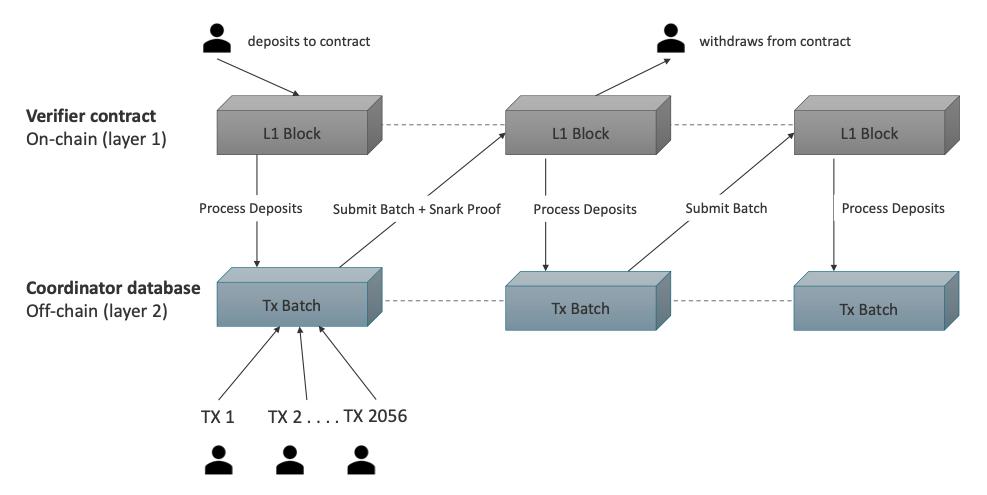
* + - Pros:
      * Faster finality time since the state is instantly verified once the proofs are sent to the main chain.
      * Not vulnerable to the economic attacks that Optimistic rollups can be vulnerable to.
      * Secure and decentralized, since the data that is needed to recover the state is stored on the layer 1 chain.
    - Cons:
      * Some don't have EVM support.
      * Validity proofs are intense to compute – not worth it for applications with little on-chain activity.
      * An operator can influence transaction ordering

The biggest problem with the Plasma approach as described above and summarize as following:

* When users want to withdraw their assets from Plasma to the Ethereum, they need to wait seven days to settle the transaction.
* Each Plasma chain requires an operator posting the Merkle root commitments to the mainchain. This requires us to trust a third party to accurately post the Merkle root commitments on the chain.
* Plasma requires that owners of transacting assets be present, and it works best for simple transfers.

1. *One of the solutions that has been gaining a lot of traction lately is zkRollups. With the use of a diagram explain the key features of zkRollups. Argue for or against this solution highlighting its benefits or shortcomings with respect to other solutions proposed or in use.*

**[ANSWER]**



Key features:

* Bundle hundreds of transfers off-chain and generate a cryptographic proof (ZK-SNARK). Then post the rollup data and proof to Ethereum blockchain for verification. The computation can be in a parallel computing model which encourages decentralization.
* Unlike Optimistic Rollup, it has no delays when moving funds from layer 2 to layer 1 because a validity proof accepted by the ZK-rollup contract has already verified the funds.
* Since the transaction and processing is handled in L2 block chain, it can extend mainchain’s scalability, increase processing speed and reduce gas fees more than 100 times.

Arguments:

* ZK-rollup is related new technology with less proven use cases compared with other L2 solutions (Optimistic rollup, Sidechains, Plasma).
* ZK-rollup relies on significant hash power to compute. Therefore, programs that have limited on-chain activity may find it more beneficial to use optimistic rollup solutions.
* ZK-compatible EVM is more difficult to build compared with other L2 solutions (Optimistic roll-up).
* Security concerns:
  + The initial setup of ZK-Rollups is assumed to be a trusted state when this trust cannot be proven. A small group of developers will be subject matter experts on the initial trusted state. This undermines decentralization and opens the risk of attacks by dishonest developer.
  + Crypto used in ZK-Snark is not quantum resistant.

However, both problems can be mitigated by ZK-STARK based ZK-Rollup, like StarkNet.

* An operator can influence transaction ordering which could cause concerns in decentralized environment.

1. *Ethereum is a state machine that moves forward with each new block. At any instance, it provides a complete state of Ethereum consisting of the data related to all accounts and smart contracts running on the EVM. The state of Ethereum modifies whenever a transaction is added to the block by changing the balances of accounts. Based on the massive adoption of Ethereum across the globe, this state has become a bottleneck for validators trying to sync with the network as well as validate transactions. Briefly describe the concept of stateless client, and how they help resolve this issue? Explain how Zero-Knowledge improves on the concept of stateless client?*

**[ANSWER]** Today, to validate a block, a Ethereum validator can be considered to validate a state transition function as: STF(current\_state, new\_block). Where current\_state is all block data and new\_block is the block to be verified. This means the validator need to load all data in local disk and replay each transaction in the new\_block. It requires lot of io and computation resources.

Stateless client is designed to make a new state transition function as: STF\_New(state\_root, new\_block, witness). Where state\_root is merkle root of the current\_state (as described above), witness is the zk-proof that prove the correct execution of transactions in new\_block. By taking this approach,

* Validator now long need to download all block data and only need to retrieve state\_root from block chain.
* The validation can be done completely in memory.

This means less disk space and io usage, and faster validation.

Zero-knowledge is key technology to enable stateless client. Specifically, ZKP can be used to:

* + - 1. Use VRF (Verifiable Random Function) and VDF (Verifiable Delay Function) to randomly select a lead validator.
      2. The lead validator uses ZK-SNARK or ZK-STARK techniques to generate proof for the correct execution of new transactions. The proof then submitted on chain.
      3. Other (stateless client) validators verify the block by just checking the proof (instead of recomputing all the transactions).

### ****Roll the TX up****

1. ***[Infrastructure Track only]*** *Review the RollupNC* [*source code*](https://github.com/rollupnc/RollupNC) *in the learning resources focusing on the contract and circuit and explain the below functions (Feel free to comment inline)*
   1. *UpdateState (Contract)*
   2. *Deposit (Contract)*
   3. *Withdraw (Contract)*
   4. *UpdateStateVerifier (Circuit)*

*Propose possible changes that can be made to the rollup application to provide better security and functionalities to the users*

**[ANSWER]**

data availability guarantees: we assume the operator will always provide data to users so they can update their leaf

circom has too many parameters is too compliated

### ****Recursive SNARK’s****