Metis DAO
Techical Fundamentals

2021 Whitepaper

INDEX

ABSTRACT

Metis aims to revolutionize how people and businesses collaborate using blockchain technology. However, layer 1 solutions such as Ethereum are struggling with high gas costs and low throughput. To achieve sophisticated collaborative outcomes and successfully deploy a framework that involves many on-chain operations requiring timely responses, a layer 2 solution is needed for Metis to achieve its mission. This paper proposes a new construct -- an optimistic rollup layer2 solution that provides both efficiency and flexibility, addressing many of the existing layer 2 solutions' problems. Metis Virtual Machine is the foundational must-have component needed to revolutionize the way people and organizations collaborate collectively and transparently in the future.

INTRODUCTION

Current DAO architecture is solely focused on efficient voting systems or governance. Metis defines DAO as a fundamental unit that supports and manages the operation of decentralized applications or businesses, we found that building trust among distrusted community members and managing decentralized collaborations are the real challenge. At Metis, we believe the future lies in the decentralized, autonomous management of day-to-day operations in a decentralized organization called a Decentralized Autonomous Company (DAC): a system entity that supports an organization's day-to-day operations, including those of large scale enterprises.

> TO BUILD A DAC THAT ALLOWS FOR COMPLEX, COLLABORATIVE OUTCOMES THAT GO BEYOND THOSE OF A STANDARD FINANCIAL PLATFORM, AN EVM COMPATIBLE OR AT LEAST TURING-COMPLETE LAYER 2 SOLUTION IS REQUIRED.
> **GIVEN THE REQUIREMENTS, THE METIS TEAM DECIDED TO ADOPT OPTIMISTIC ROLLUP AS ITS LAYER 2 INFRASTRUCTURE.**

PROBLEMS

Currently, here are some significant issues with many popular optimistic rollup layer 2 solutions:

1. The standard layer 2 design is usually very centralized. Many of these constructs duplicate a centralized structure from a single sequencer, which rely on the verification mechanism to deter malicious players from fraudulent behaviors. This design leads to the second problem.

2. It usually takes a long time to finalize a transaction. Especially when there is a need to withdraw from the layer 2 construct to layer 1. The time to finalize the transaction can take many days.

3. This, in turn, will cause a bottleneck on layer 2 again. Because of the

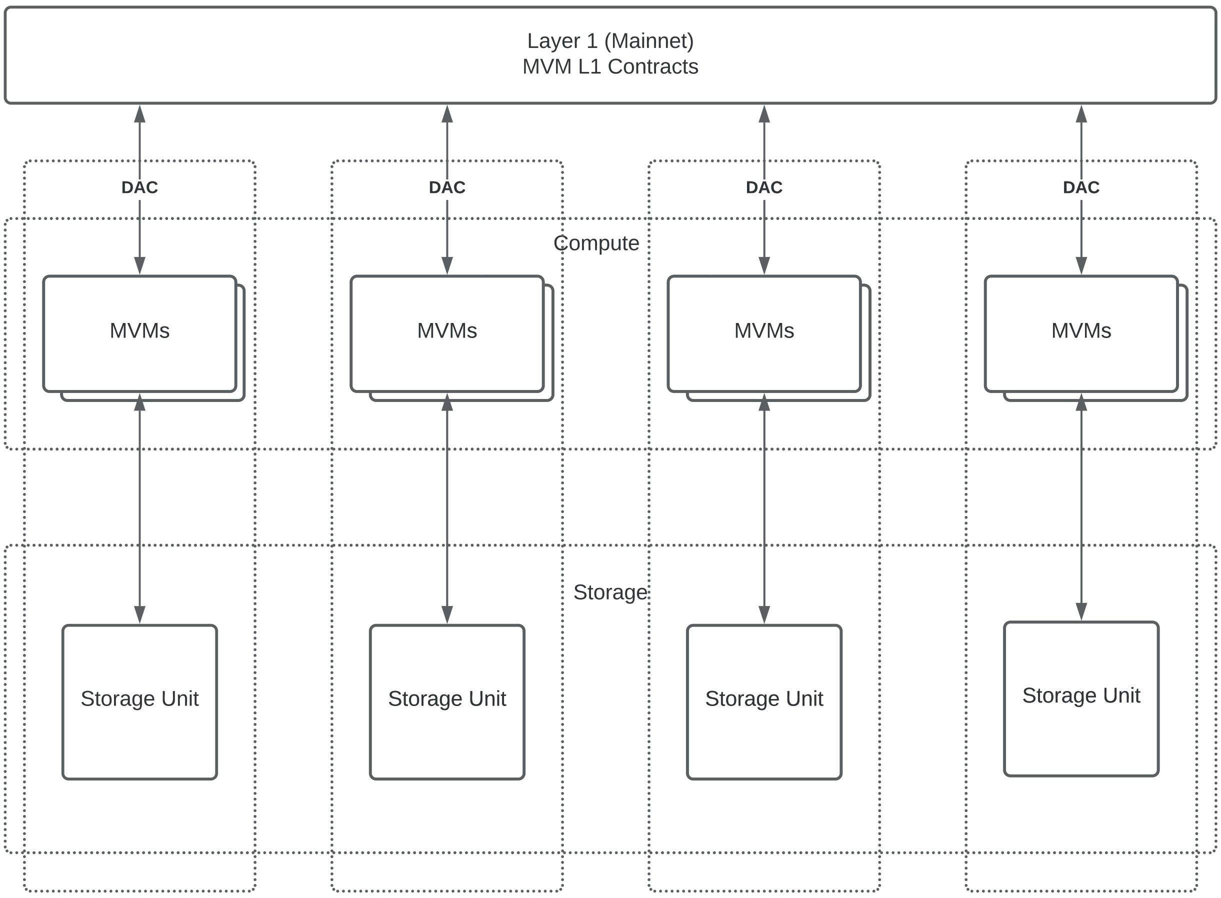
way many layer 2 solutions are constructed, the throughput on Layer 2 will eventually be limited by the centralized stack's power. If the goal is to bring DApps to the mainstream, we must allow the layer 2 solution to scale.

To solve those issues and meet the rising demand for DAC operations, Metis designed and implemented a new layer 2 solution with an EVM-compatible virtual machine called the Metis Virtual Machine or MVM. The following sections highlight many of the new design features that make the MVM stand out amongst other layer 2 solutions.

SEPARATE OF COMPUTE AND STORAGE FOR ULTIMATE SCALABILITY.

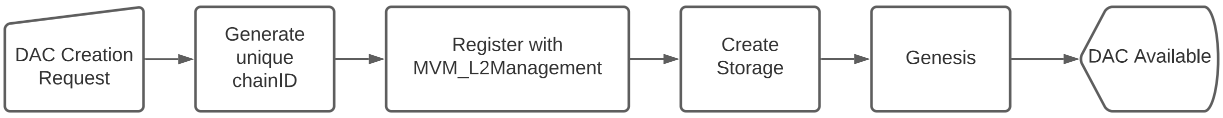
In MVM, each Decentralized Autonomous Company (DAC) is associated with a unique layer2 construct where all DAC collaborations occur. MVM separates the computing and storage of the Ethereum construct for layer 2. More specifically, a DAC creation only triggers the creation of a new storage layer specifically for that DAC. The computing part, including block mining and cross-layer communications, is scaled up and down dynamically on-demand as part of the Metis system. It is a crucial design highlight to allow Metis to scale horizontally without incurring significant spending in infrastructure. The income from economic activities within each DAC will be able to cover the infrastructure cost easily.

Furthermore, MVM allows providers to sign up and contribute computing power to make layer2 construct truly decentralized. The provider will be incentivized based on the blocks produced. The key point is that the provider may not know which DAC will be worked on. It helps make sure that there won't be targeted attacks by malicious computing power providers



As part of the MVM design, L1 contracts know how to handle state roots, transactions and proposals from different L2 contracts. Every transaction batch and state roots also have a chainID attached to the payload. The chainID is a unique identifier for each layer 2 construct and is also used for signing transactions across the layers.

When a DAC needs to be created, as part of the Comco protocol, a smart contract on the layer 1 will generate a unique chainID for the new construct, register with the Metis management smart contract and trigger the deployment of the storage units by Metis microservices.



Each DAC will be assigned to a unique subdomain name under metisdao.org, where users will be able to interact with DAC via the subdomain name directly.

DAC CHARTER TO GOVERN THE OPERATION RULES

Like organizations in the real economy, a DAC also has a charter to set its fundamental operating rules. MVM_DACMaster is a smart contract that dictates the operations of the DAC on MVM layer 2. The smart contract is part of the genesis block and includes the following important information about the DAC:

1. **vision:string and mission:string** – purpose of the DAC

2. **permissions:{address:string[],** operation:string, opcode:string}[] – a set of addresses that can perform certain operations on MVM Layer2 including basic read/write access.

3. **taxrates:{threshold:int, rate:int}[]** – define the mechanism how the transactions within the DAC are taxed.

4. **management_contract:address** – define the process of changing the content of the DAC Charter such as DAO-like voting mechanism or simply being immutable based on the smart contract set.

The charter will be created during the genesis. The initial settings will be finalized in the first block after genesis and as part of the DAC creation process. The management contract will be the only signer that can modify the charter afterward. The only exception is the tax rate, which Metis, managed by MetisDAO, can set.

MVM LAYER 2 PERMISSION MANAGEMENT

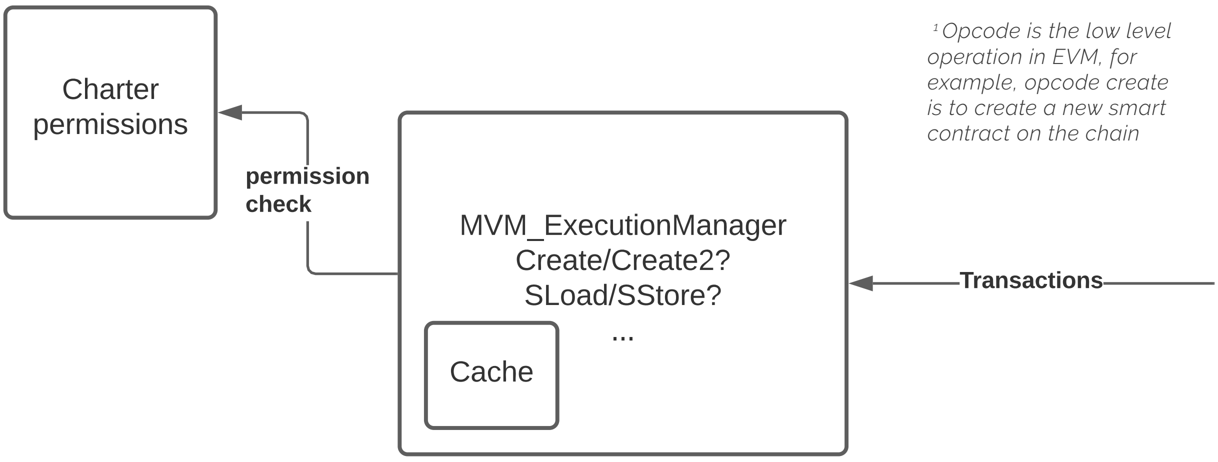
In any organization, structure and permissions are two important factors that govern the effective operation. As part of the MVM, we introduce a flexible permission system that can manage the access to a particular layer 2 DAC as granular as on the opcode level.

In the DAC Charter, each opcode is associated with a list of addresses that are allowed or prohibited to execute the opcode as part of the execution. MVM_ExecutionManager, which is responsible for executing opcodes, checks the permissions before executing the opcode. Extensive caching is implemented to minimize the impact of permission check during the execution. Some examples of permission implementations include but not limit to:

1. **Only a small subset of signers can deploy smart contracts** – this can allow the DAC to have better control of its own ecosystem including token distribution.

2. **Only the DAC participants are allowed to submit transactions** – this configuration can create a permissioned DAC.

3. **A subset of signers are banned to submit transactions** – in this way, DACs can blacklist toxic members or malicious users.

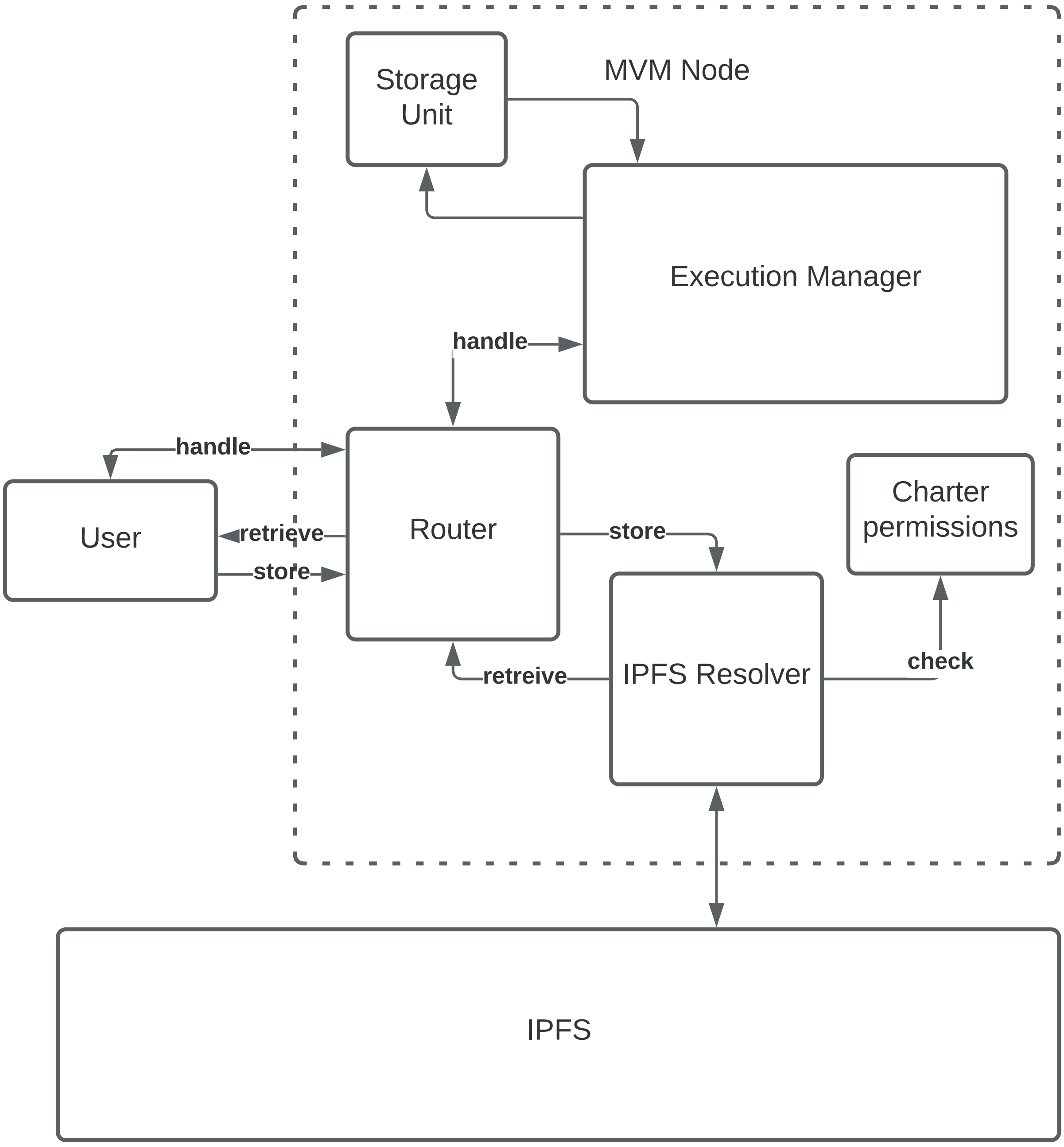


[1] Opcode is the low level operation in EVM, for example, opcode create is to create a new smart contract on the chain

LASTLY, THE PERMISSION LAYER IS TOTALLY OPTIONAL. MVM CAN STILL BE A PERMISSIONLESS LAYER 2 CONSTRUCT.

SPECIAL STORAGE LAYER BASED ON IPFS TO MANAGE CONFIDENTIAL DATA.

Another important piece of the puzzle is MVM's special storage layer. MVM has a regular storage layer to store blocks and states. However, for some DACs, there will be sensitive information that they don't want to be public outside the DAC. Because all transactions are packaged to L1 for potential dispute scenarios, confidential data on the blockchain will still be accessible outside the DAC. Encryption is often adopted as a solution for this challenge. However, the encryption and decryption operation would require a centralized service manager and provide access to the encryption key pairs. Here at Metis, we decided to use IPFS to solve the problem.



THERE ARE A NUMBER OF IMPORTANT CONSIDERATIONS.

1. The IPFS cluster is only accessible through the IPFS resolver on MVM Layer 2. The access to IPFS resolver can be controlled via Charter permission rules. The IPFS resolver on each layer 2 chain carries a unique key to encode the identifier so that other layer 2 DACs will not be able to access confidential data.

2. To remain compatible with most existing clients, the user will invoke methods via the same node as regular transactions that handle most common functions such as signing checks. MVM's IPFS router will intercept IPFS related operations so that those operations are not included in the rollups.

3. IPFS transactions are not rolled up to L1, otherwise, the purpose of having a special storage layer is defeated. However, the user is supposed to save the file handle in the smart contract. The transaction to save the handle is a regular transaction that will be rolled up and ready for fraud proofing challenges. Because saving the handle doesn't affect other states, the fact that L1 doesn't have access to the IPFS cluster does not affect fraud proofing.

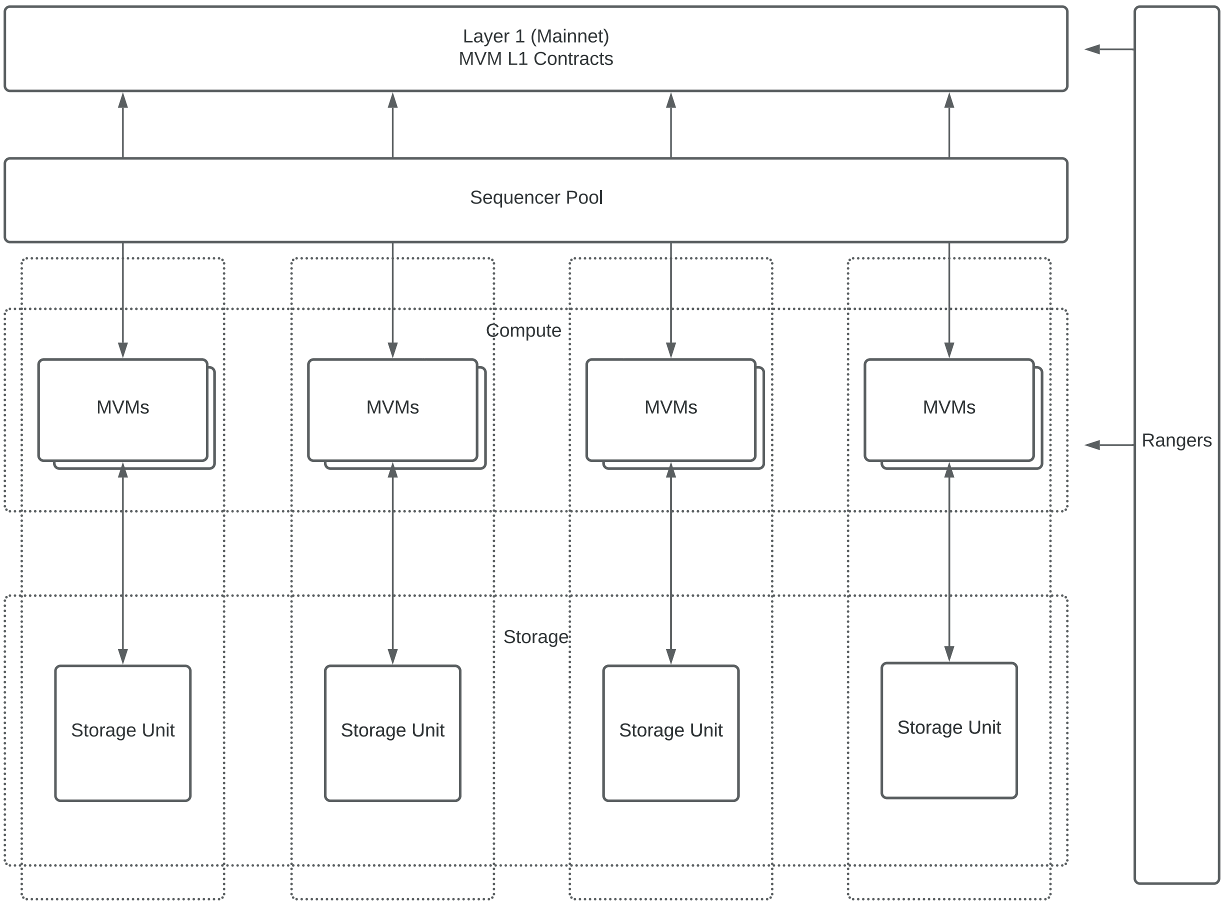
SIGNIFICANT REDUCTION OF THE FRAUD PROOFING WINDOW

Among all rollup solutions, fraud proofing is always part of the trade-off. Optimistic Rollup usually comes with a long fraud proofing window to give Rangers enough time to validate the state roots. The long window makes withdrawal to L1 much less efficient. As part of MVM, we aim to minimize the fraud proofing window by decentralizing the rollup process and pushing down the state root validation.

Based on the work, which separates the computation and storage, the rollup process will no longer be handled by a single sequencer. A pool of sequencers will be randomly selected to Rollup the state roots and submit the transactions.

Furthermore, MVM introduces a unique role called L2 Ranger. L2 Rangers are members of a special DAC called MVM_RANGERS. Rangers are able to sample a range of blocks and validate the state roots according to the transactions assigned periodically from a random DAC, including MVM_RANGERS itself. Each completed validation will result in an incentive in MT, which can be withdrawn to L1 if the validation spots a discrepancy and the challenge process will automatically start. A successful challenge will award the validator a portion of the bond. A failed challenge will cause the validator to lose the bond and eventually lose access to **MVM_RANGERS.**

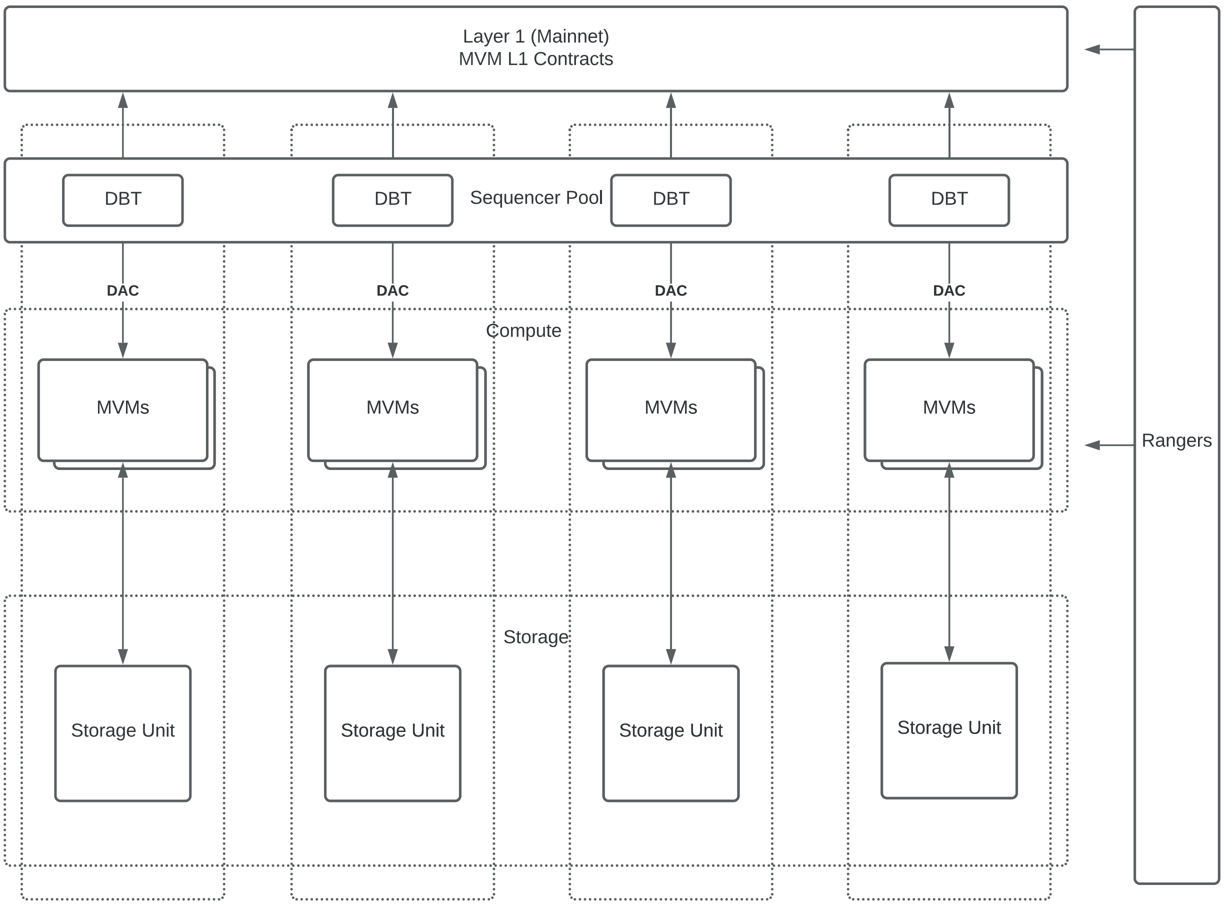
All the above work is to make the arbitration game fairer and more attractive to the rangers. With both decentralized sequencing and a healthy pool of L2 rangers, MVM will greatly shorten the required proofing window to enhance network efficiency further.



DYNAMIC SEQUENCER BONDS TO SAFEGUARD THE NETWORK

Another essential mechanism to deter malicious sequencers from fraudulent behaviors is the bond. Each sequencer needs to stake a number of Metis Tokens to be qualified. However, the Metis ecosystem has strong, real economic connections, with transaction value that can be in the billions. The risk and reward of malicious behavior starts to tip towards the more dangerous side. Thus, MVM introduces a concept called the Dynamic Bond Threshold (DBT).

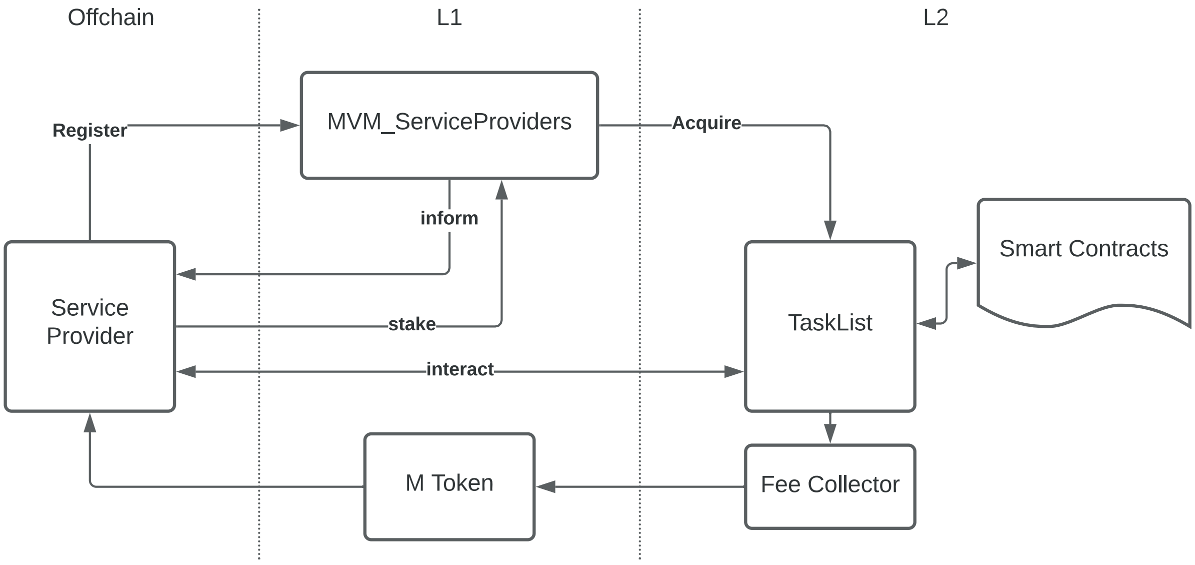
DBT is calculated based on the maximum economic capacity of a given DAC, i.e., the total supply of MVM_Coinbase. If the number of staked Metis Token of a particular sequencer is below the DBT of a DAC, the sequencer cannot partake in the DAC sequencing work. When an MT deposit and withdrawal operation executes, the DBT will automatically be updated. If none of the sequencers in the sequencer pool are eligible after a deposit operation, the operation will be blocked until an eligible sequencer is found.



INFINITE EXPANSION WITH MICROSERVICE FRAMEWORK.

MVM supports the basic principles of microservice framework. Providers such as oracles, delivery service, or legal can register as a microservice provider in the MVM ecosystem. They serve as toolkits to all DACs to help fulfill the mission and visions. MVM supports automatic payment collection. The service providers will be given an SDK to easily interact with the smart contract on any Metis Layer 2 constructs, including payment collection, to lower entry barriers. It allows service providers that are not familiar with blockchain technology to join the ecosystem.

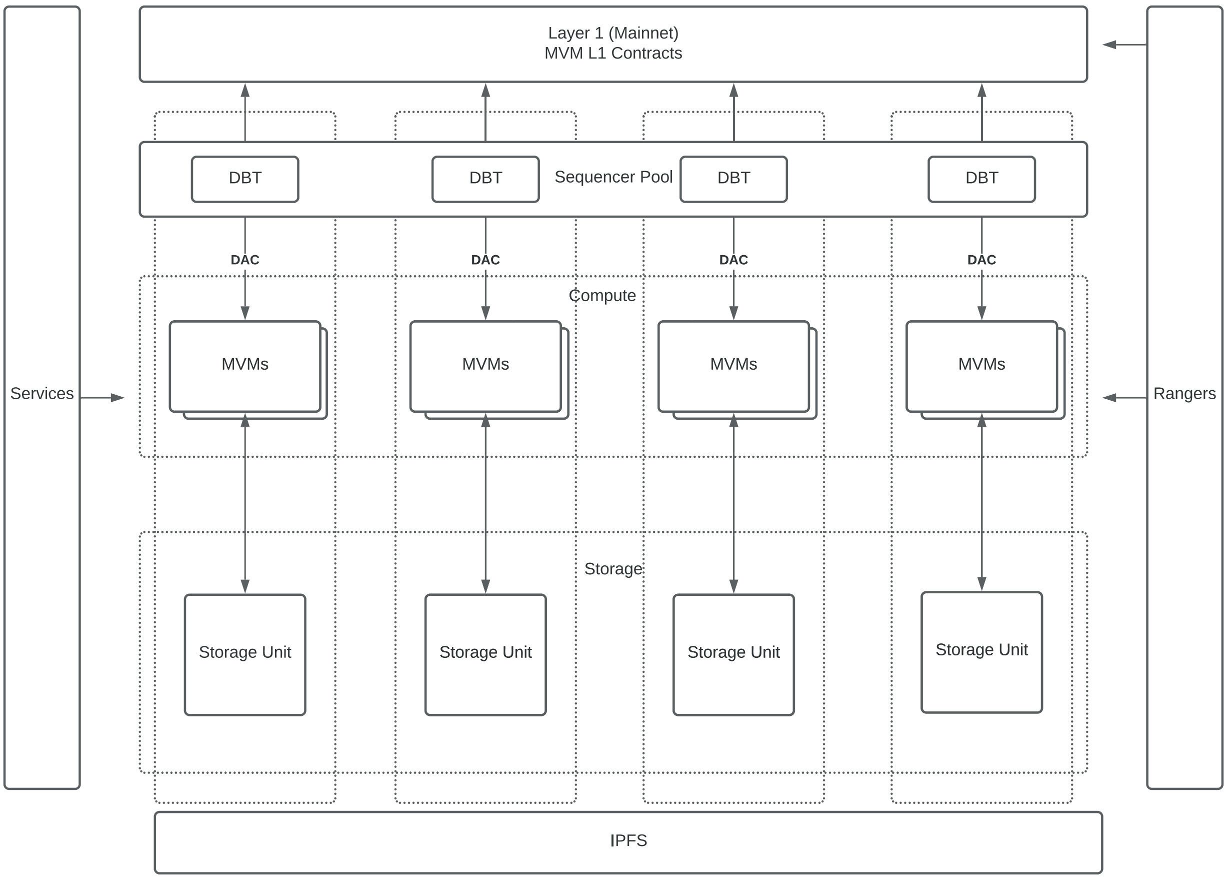
THIS ARCHITECTURE ENABLES INFINITE EXPANSION OF SERVICES AVAILABLE IN THE MVM ECOSYSTEM AND A CRITICAL PIECE TO CONNECT THE OFFCHAIN ECONOMY WITH THE BLOCKCHAIN ECONOMY.



SUMMARY

With sequencers, block producers (compute), IPFS cluster provider, service provider and rangers, MVM solves the most pressing issues with many popular layer 2 solutions and builds a system that is both highly efficient and also well decentralized.

Powered by MVM, Metis creates an ecosystem to build a truly decentralized economy based on layer 2. We believe this is the future of organizations, communities and the economy.



METIS

METISDAO.ORG

Metis DAO

Techical Fundamentals

Version 1.0

Last Revision Mar 2021