Setheum Network: A Secure Confidential And Interoperable Decentralised Cloud Compute And Storage Network With A Layer-2 Infrastructure for Subchains and Smart Contracts

Technical White Paper - v15

MAY 2023

By

Muhammad-Jibril B.A. (Khalifa MBA)

Founder, Chief Architect, Grand Imam

Slixon Technologies | Setheum Labs| Open Web3 Foundation

Abstract

The intent of the Setheum Network is to improve upon Web3 and solve the blockchain trilemma with a mixture of approaches and a recipe formed from what we have seen and considered to be some of the best solutions in the field, improving on scalability, security, mass adoption, diversity, and ethics while preserving decentralisation and democratisation.

We see a lot of blockchains coming up, yet we haven't seen many that have either solved the trilemma or effectively found reasonable equilibrium in the trilemma thus achieving a decent level of scalability, increased network security and a decent level of decentralisation. Setheum intends to be just that and more, it intends to be the most scalable blockchain network in the world while providing confidentiality for Subchains(Sidechains natively built into the network) and Cloud Computing and Storage Infrastructure for Web3 based Internet Solutions and Interoperability with both Web2 and other Web3 Networks.

Setheum is being built along with its first Subchain named "Khalifa", after Me, to signify its efforts and approach towards building Ethical DeFi Solutions. Khalifa Blockchain is designed for EVM-compatibility and optimised for DeFi, built on Setheum's native STEM (Setheum Trusted Execution Machine; built on TEEs) + DAGESTAN (Directed Acyclic Graph Engine for Succinct Trustless Asynchronous Networking; built using ABFT) Stack to make it the most scalable blockchain in the world.

With Setheum's STEM, teams can build Subchains just like the Khalifa Subchain leveraging all the functionalities and features of the Setheum Network and having hardware level shared security across the network. Subchains can be private, public or consortium, they can be permissioned or permissionless, they can be anything the builders want it to be.

The Setheum STEM-DAGESTAN architecture powers the network to be the most scalable blockchain in the world; it enables near instant finality, high throughput, linear scalability and interoperability for the Setheum Network. However Subchains can choose to use any other combination on the STEM architecture (eg. STEM-GRANDPA, where GRANDPA is the consensus finality gadget instead of DAGESTAN's Finality Gadget) they can decide on using any other Consensus Mechanisms other than DAGESTAN-Based Consensus.

Table of Contents

Introduction

Setheum achieves a high level of equilibrium in the trilemma by leveraging a Directed Acyclic Graph(DAG) to build the blockchain consensus making it a Blockchain via DAG, achieve instance finality, high throughput and subsecond blocktime while preserving network security and having a fairly decentralised network, Setheum's consensus system leans towards achieving high scalability and high security with an ethical, decent and equitably high level of decentralisation.

Setheum is EVM(Ethereum Virtual Machine) compatible for smart contracts to thrive on its super fast blockchain, the entire chain is upgradable and forkless enabling forkless upgrades as Setheum is built with the Substrate framework using the Rust programming language. Khalifa's DeFi Suite powers the Ethical DeFi revolution on Setheum, being on the fastest public blockchain network in the world and leveraging all the benefits that come with being on Setheum, making it a DeFi optimised blockchain especially exceptional for DeFi applications and solutions.

Khalifa Subchain's DeFi Suite is also the DeFi powerhouse of the Setheum Network, providing all kinds of top notch DeFi protocols including an AMM DEX, payment gateway rail based on setheum's built-in payments modules, DEX aggregator, Decentralised Liquid Staking for for both Setheum SEE and Khalifa KHL and ethical zero-interest halal stablecoins that gives us the properties of both Fiat and Crypto with SlickUSD (USSD), and Setter (SETR) using an Ethical Collateralized Debt Position (ECDP) mechanism that is over-collateralized and multi-collateralized and stable without compromising decentralisation or economic stability, offering zero-interest loans of stable cryptocurrencies that has scalable value and trust, setheum provides just that, backed by crypto assets with efficient zero-interest loans.

Brief History

It all started in 1976, cryptographers Whitfield Diffie & Martin E. Hellman published their paper “New directions in cryptography”. David Chaum first proposed a protocol similar to Bitcoin in his thesis "Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups.” in the year 1982. Then S. Even, O. Goldreich, and Y. Yacobi published “Electronic wallet” later in 1983. Furthermore, since then we’ve seen inventions in this field being introduced by some of the most brilliant minds around, this gradually builds up and leads to what we know today as the “Blockchain” In 1998 yet again, Nick Szabo introduced the design of a mechanism for a decentralised digital currency he called "Bit Gold". Though Bit Gold was never implemented, it has however been dubbed "the direct precursor to the Bitcoin architecture.” In Nick Szabo’s Bit Gold, a participant would dedicate computing power to solve cryptographic challenges (like puzzles). In the Bit Gold network, solved cryptographic hashes would go through a BFT (Byzantine Fault-Tolerant) public registry and be assigned to the public key of the participant/solver. Each solution would become part of the next challenge, creating a growing chain of new challenges. This provided the Bit Gold network with a method to verify and time-stamp new Bit Golds, because unless a majority of the validation participants agree to accept new hash solutions, they couldn’t start on the next challenge. When attempting to design a digital currency, challenges like the "double-spending" problem arise. Once data has been created, reproducing it would simply be a matter of copy and paste. Most digital currencies would solve the problem by advocating some control over to a central authority, which keeps track of the account balances. This was clearly an unacceptable solution for Nick Szabo, "I was trying to mimic as closely as possible in cyberspace the security and trust characteristics of gold, and chief among those is that it doesn’t depend on a trusted central authority,"said Szabo. The phrase and concept of "smart contracts" was also developed by Nick Szabo, with the goal of bringing what he calls the "highly evolved" practices of contract law to the design of trustless e-commerce protocols on the Internet. More papers were published to achieve fairly the same objective, a peer-to-peer trustless and secure electronic monetary equivalent. All these inventions were neglected and almost forgotten until when we needed them the most in the 2007-2008 financial crisis, what a crash, I had wish we saw the black swan coming earlier and took all preventive measures, but we just simply didn’t trust crypto, and now it’s proven us totally wrong, though it hurts to be wrong we have to admit we must transition to a better economic stability strategy. On the 7th of April 2008, MICHAEL NÜSKEN published “WORKSHOP e€ (ELECTRONIC MONEY).” In the same catastrophic 2008, Blockchain was invented by a person under the alias of “Satoshi Nakamoto”, to serve as the public transaction ledger of the cryptocurrency “Bitcoin”. The identity of Satoshi Nakamoto remains unknown till date. The invention of the blockchain for the bitcoin network, made it the first digital currency to solve the “double-spending” (where one could spend a unit of exchange more than once) problem without the need for a trusted centralised authority. The bitcoin design has inspired many other applications and blockchains that are public, transparent. The blockchain is considered as a type of payment rail. Late 2019, I proposed Setheum and its Subchain Khalifa to serve the underserved in this industry and introduce an ethical shari’ah compliant Blockchain and a group of protocols.

Understanding The Blockchain

The blockchain is a decentralised, electronic ledger made up of **blocks** used to record transactions across distributed nodes such that any recorded block cannot be altered retroactively, without the alteration of all the subsequent blocks. This enables the participants to verify and audit transactions independently. A blockchain's database is managed autonomously using a peer-to-peer network and a distributed timestamping server. They are authenticated collectively by participants with similar self-interests. The blockchain does away with having to trust a central authority or server, making it trustless and it is transparent to support auditing and ensuring readability.

- 1st Generation - Bitcoin (Cryptocurrency)

The 1st generation of the blockchain aimed at Cryptocurrency is the first implementation of distributed ledger technology (DLT). This allows financial transactions based on blockchain technology or DLT (for the sake of simplicity often seen as synonyms) to be executed with Bitcoin being the most prominent example in this segment. It is being used as A STORE OF VALUE, a digital payment system and can be seen as the enabler of an "Internet of Money".

- 2nd Generation - Ethereum (Smart Contracts)

Ethereum blockchain aims to execute 'Smart Contracts' to reduce the cost of verification, execution and fraud prevention. They are independent computer programs that automatically execute predefined conditions. A DApp can have frontend code and user interfaces written in any language that can make calls to its backend, like a traditional App. But a Dapp can have its frontend hosted on decentralised storages such as Ethereums Swarm. ***[****DApp = frontend + contracts* **(**running i.e. on Ethereum**)]**

- 3rd Generation and Web3.0 (leapfrog)

The first generation of the Blockchain aims at solving the issue of double-spending and providing a decentralised and secure monetary system on the internet, and this is where Bitcoin lands as the first successful implementation of decentralised finance. The Second generation focuses on the programmability of the blockchain layer, to support a diverse range of application development on the blockchain, and that is when Ethereum was introduced that supports an EVM (Ethereum Virtual Machine) which is a programmable layer on the blockchain that allows the deployment of smart-contracts that can interact with each other on top of the blockchain.

The 3rd generation blockchain revolves around the idea of interoperability and the 3 Ss namely **sustainability**, **scalability**, and **security**. This is where we see Proof of Stake implementations that are environmentally friendly and an alternative to the legacy "Proof of Work" for long-term environmental sustainability with works like Polkadot and Setheum. Here we see decentralised storage like Filecoin, IPFS, and Chia that use Storage Consensus mechanisms. Here we see state upgradability without forking like in Polkadot and **Setheum**, we see on-chain built-in DeFi systems like in the case of Setheum. We also see layer 0 solutions like Polkadot and layer 2 solutions alongside many innovations in the blockchain and crypto space.

Inspiration & Motivation

- The **Inspiration** behind Setheum was initially to provide an alternative payment system to the current FinTech atmosphere. To create a system that is bipartisan and open to the public providing an easy to use remittance network that is also easy to onboard, attractive for day-to-day spending and transparent. Something I could build an ecommerce platform on and use as the main payment option to accept crypto payments and build a bridge between traditional finance and cryptocurrency in both low-level and high-level endpoints, deploy my full stack backend+frontend on the blockchain without paying transaction fees for every computation token, and store my database on network, especially in the less developed and developing parts of the world.
- The **motivation** is to make it easier for the free-flow of capital internationally and intersystemic, to maximise and power Open Web3 Solutions (Blockchain + Compute Cloud + Storage Cloud).

Setheum Network

Setheum is cloud optimised Web3 operating system, Interoperability Focal Point, and Communication System that resolves around the issues of the **Blockchain Trilemma**, enabling smart contracts, confidential hardware-level shared-security blockchains (**Subchains**), confidential computing, confidential smart contracts and intersystemic interoperability. Setheum is built with the **Substrate** modular interoperable blockchain framework. In Setheum, one can pay for transaction fees in any token currency powered by **KhalifaSwap** without having to hold Setheum's native token. Setheum implements a free and fair economic system that pursues equality of opportunity and the maximisation of public utility in the crypto-economy.

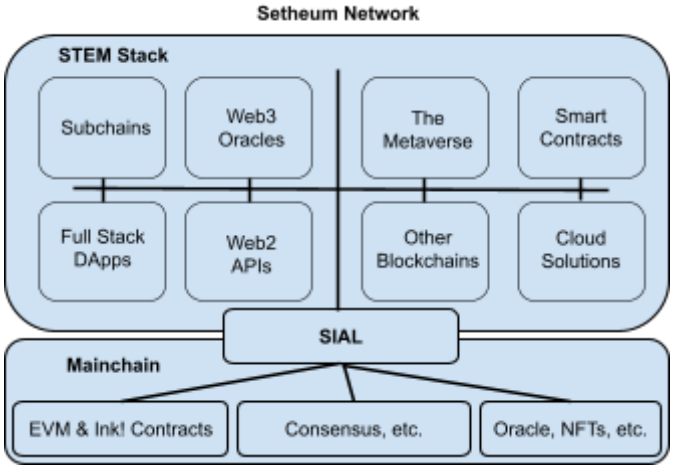

Fig-1: Setheum Network Architecture Abstraction

The 5 Pillars of the Setheum Network

There are Five (5) Pillars to the Setheum Network that are crucial parts of the Network, these 5 pillars complete the network. The 5 Pillars Setheum are inspired by the 5 Pillars of Islam, but it describes the technical pillars of Setheum not religious or philosophical pillars, looking into what are the 5 most important building blocks of the Setheum Network. These 5 pillars give the network the shape of a pentagon, these pillars are as follows:

1. **CPoW and CPoS** (Cloud Proof of Work & Cloud Proof of Stake)
2. **DAGESTAN** (Directed Acyclic Graph Engine for Succinct Trustless Asynchronous Networking)
3. **SIAL** (Setheum Interoperability Actuation Layer)
4. **STEM** (Setheum Trusted Execution Machine)
5. **Khalifa Subchain** (Ethical DeFi)

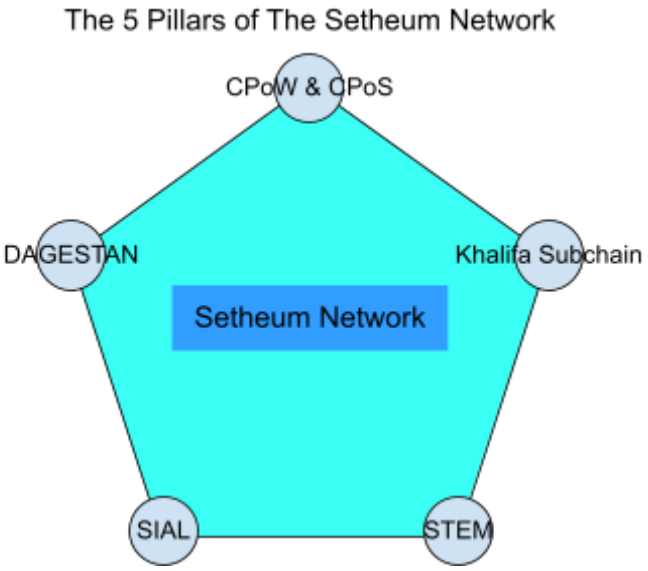

Fig-2: The Five (5) Pillars of the Setheum Network

The 6 Corners of the Setheum Ecosystem

There are Six (6) Corners to the Setheum Ecosystem that are crucial parts of the Ecosystem, they complete the ecosystem and define its values and core ingredients of the ecosystem. The 6 Corners of the Setheum Ecosystem are inspired by the Six (6) corners of belief in Islam, but they are describing the technical corners of the Setheum Ecosystem and not religious or philosophical corners, these 6 corners give the Setheum Ecosystem a hexagonal shape. These corners are as follows;

1. **Khalifa DeFi Protocols** (Ethical DeFi)
2. **Mainchain & Subchain** Stack
3. **Cloud Stack** (Compute Cloud and Storage Cloud)
4. **Smart Contract Protocols** (ie. Ink! And EVM Smart Contracts)
5. **Wallet Recovery** Protocol
6. **Native Assets** (ie. SEE)

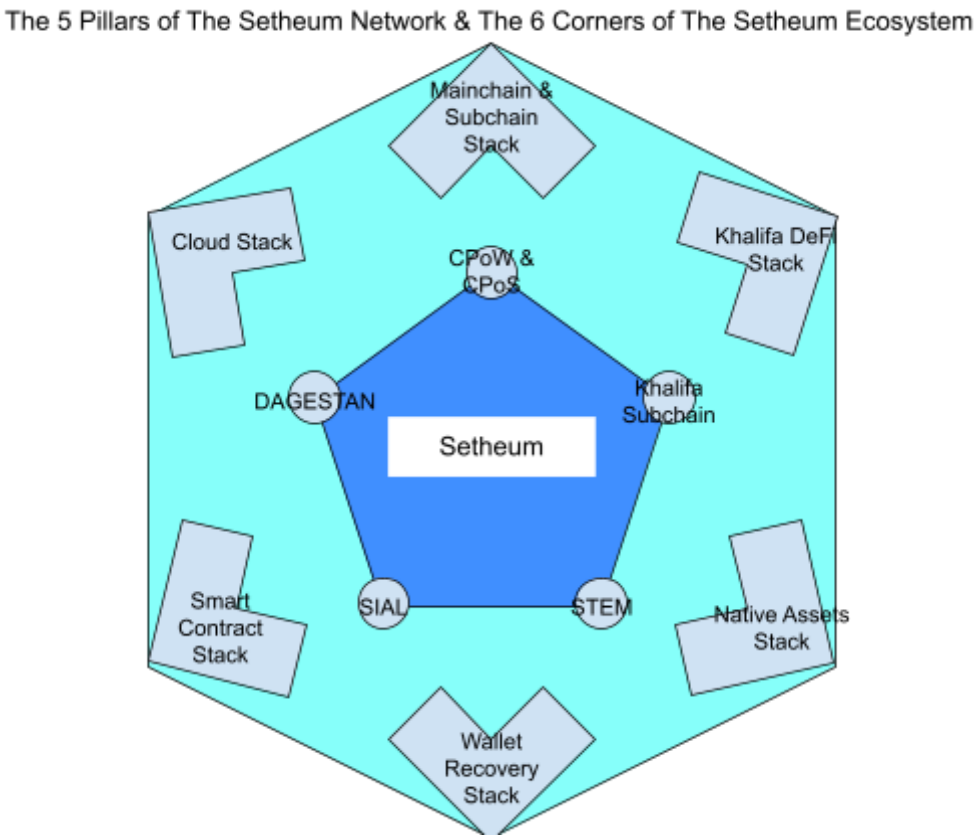

Fig-3: The Six (6) Corners of the Setheum Ecosystem

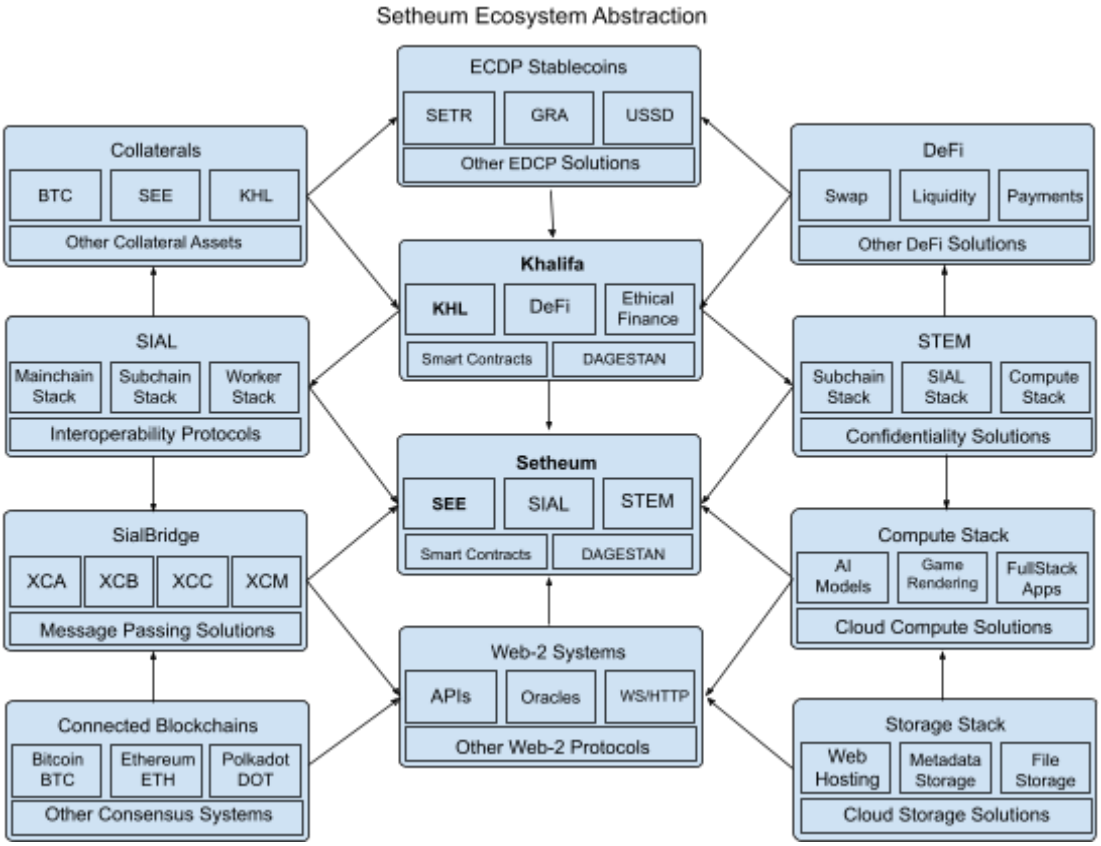

Fig-4: Setheum Ecosystem Abstraction

Participants Involved in the Setheum Network

There are two types of participants mentioned here, the Setheum Network `Participants` and `Nodes` who participate in operating the network from cloud resources provision down to network consensus.

Network Entities

1. **Provider:** This participant takes part in providing cloud resources (compute and storage) to the network, they are the `StandardProvider` and `PoolProvider`.
2. **StandardProvider:** The `StandardProvider` is a `Provider` that also serves as a `validator` for the network, providing cloud resources as well as participating in consensus.
3. **ProvisionPool:** A `ProvisionPool` is a group of pooled cloud resources brought together to participate in cloud provision in the Setheum network as a `Provider`. A `ProviderPool` has a `PoolProvider` who is a member of the pool, and a `PoolValidator` who creates the pool and is the owner of the `ProvisionPool`.
4. **PoolValidator:** The `poolValidator` is a provider that initiates and owns a `ProvisionPool` that members/providers can join to pool their provider resources together, the `poolValidator` only acts as the owner of the `ProvisionPool` as well as a `Validator` participating in the network consensus and thus is not a `Provider`. The `PoolValidator` enjoys the benefit of having a larger `StakingQuota` due to the pooled resources of its `ProvisionPool`.
5. **PoolProvider:** The `PoolProvider` is a provider that participates in providing cloud resources to a `ProvisionPool`.
6. **Validator:** The `Validator` is responsible for producing, verifying and validating blocks for the consensus of the network, they are the `Verifier` and the `Candidate`.
7. **VerifierValidator:** The `VerifierValidator` is a `Validator` in the `ActiveValidatorList` that actively takes part in the network's block production, verification and validation.
8. **CandidateValidator:** The `CandidateValidator` is a `validator` that is not elected in the `validator-election` to be a `VerifierValidator`, it stays as a `candidateValidator`for the period that its not a `verifierValidator`.
9. **Nominator:** A `Nominator` is a user that stakes on the network via nominating a provider or providers without being a provider itself. A nominator can nominate up to 16 validators.
10. **Node:** A node is an instance/computer of the network that participates in running the network as an operator. All the computers that run as network participants such as the `Validator` and `Provider` are nodes of the network. The Setheum network connects these nodes together as a peer-to-peer network.

11. **CloudWorker**: A `CloudWorker` in Setheum is a STEM off-chain computation `node` with cloud capabilities that provide cloud resources to the network in STEM enclaves.

Network Nodes

There are many types of nodes in the Setheum Network, all of them are listed and explained below. Setheum Nodes are classified into two, the `mainchain-node` and the `subchain-node`.

- Mainchain Nodes: Nodes participating on the L1 `mainchain` of the Network.
  They are Five (5) and listed below:
  1. `archive`: This RPC node archives all the `mainchain` on-chain storage.
  2. `light`: This node runs a `mainchain` `LightClient`.
  3. `standard_provider`: This node runs a `mainchain` `standardProvider`.
  4. `pool_validator`: This node runs a `mainchain` `PoolValidator`.
  5. `pool_provider`: This node runs a `mainchain` `PoolProvider`.
- Subchain Nodes: Nodes participating on the L2 `subchain layer` of the Network.
  They are Three (3) and listed below:
  1. `archive`: This RPC node archives all the `subchain` on-chain storage.
  2. `light`: This node runs a `subchain` `LightClient`.
  3. `Validator`: This node runs a `subchain` `Validator`.

DAGESTAN Consensus Engine

Directed Acyclic Graph Engine for Succinct Trustless Asynchronous Networking

DAGESTAN is Setheum's native consensus engine built as a blockchain-DAG system built using AlephBFT consensus mechanism. Setheum's finality protocol for consensus is called Dagestan Finality Gadget based on the DAGESTAN consensus engine. The finality is expected to be near instant. Setheum uses BABE for block authoring, DAGESTAN for finality, ***Cloud Proof of Work (CPoW)*** for Cloud Compute and Storage Resourcing, and ***Cloud Proof of Stake (CPoS***) for staking. DAGESTAN is an Asynchronous BFT consensus protocol, which allows distributed systems to reach consensus on the state of the network, even in the presence of malicious or faulty nodes. The BFT algorithm uses cryptographic signatures and other security mechanisms to ensure that the consensus reached by the network is both correct and tamper-proof. DAGESTAN is specifically designed to be efficient and scalable, making it suitable for use in large-scale distributed systems, like blockchain networks such as Setheum.

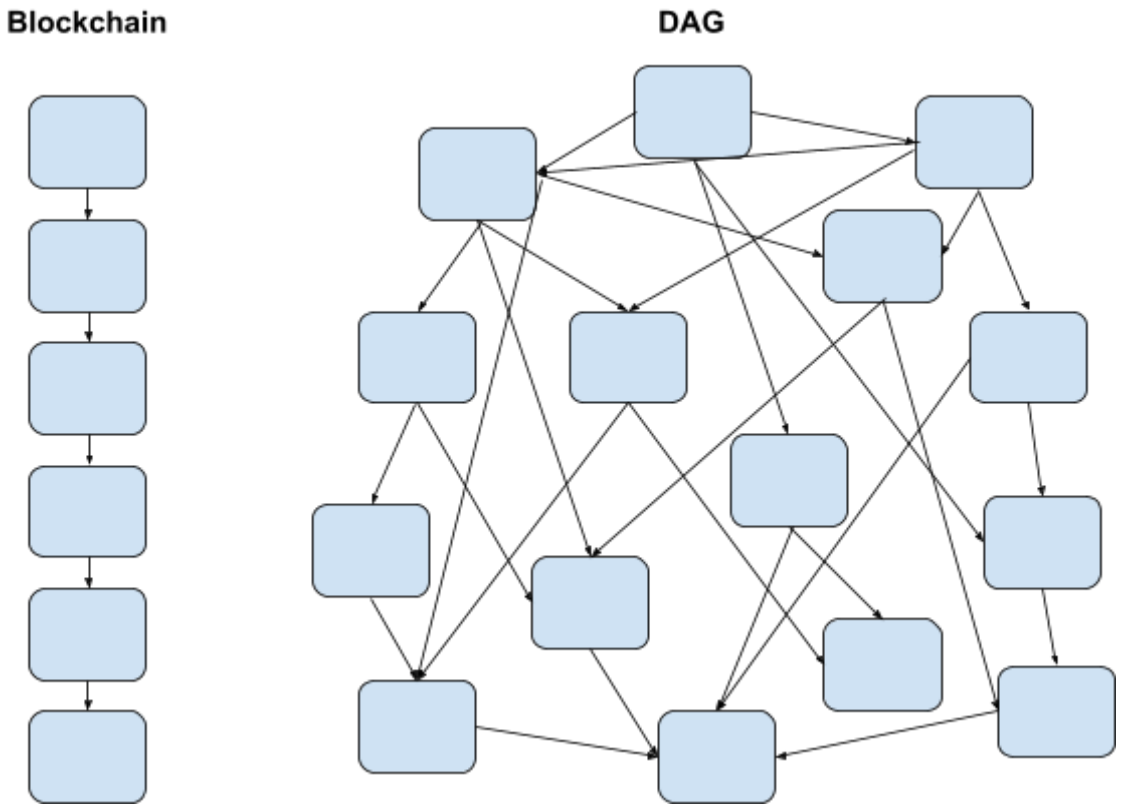

Fig-5: Blockchain vs DAG Architecture

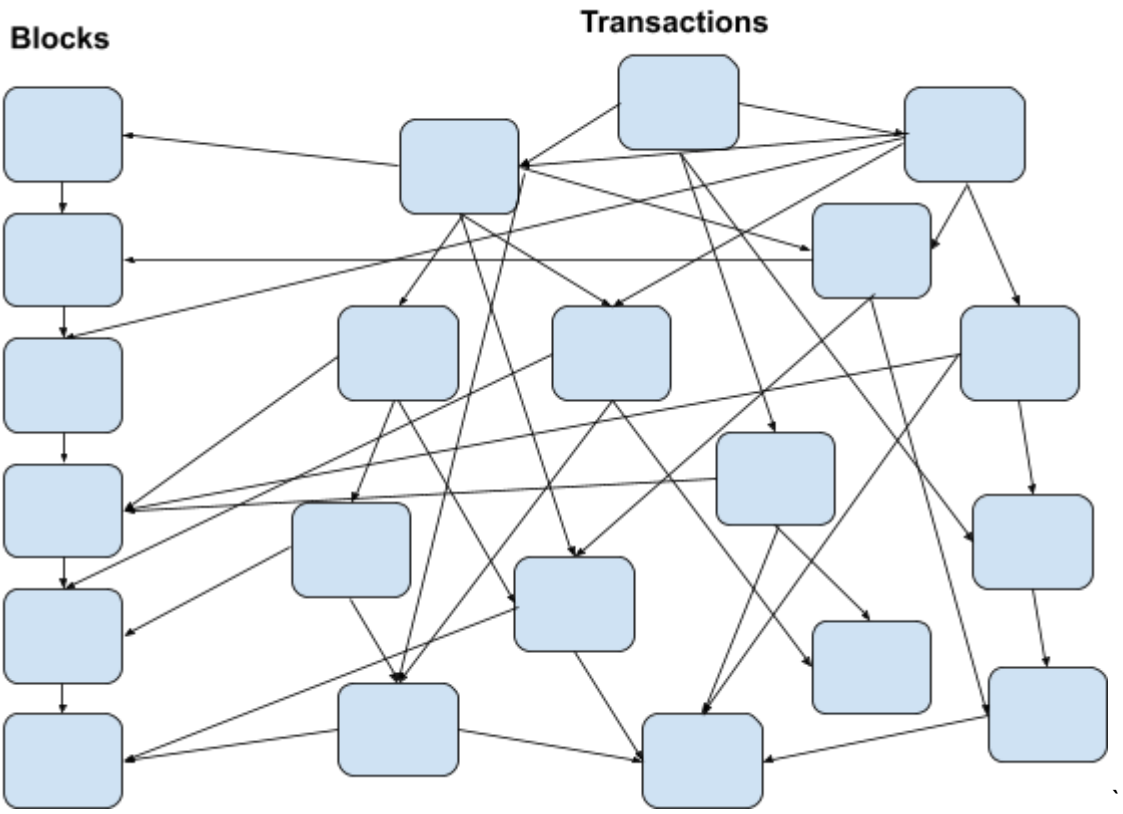

Fig-6: DAGESTAN Architecture

The DAGESTAN protocol uses a sharding approach, where the network is divided into multiple shards, each of which can reach consensus independently. This allows the protocol to achieve high throughput and low latency, while still maintaining security and fault tolerance.It is designed to be efficient and scalable, with near instant finality, and is able to ensure that the consensus reached by the network is both correct and tamper-proof, even in the presence of malicious or faulty nodes. A DAG, or directed acyclic graph, is a type of graph in which the edges have a direction and the graph does not contain any cycles, or loops. This means that it is not possible to traverse the graph and visit the same vertex more than once when following the direction of the edges. With DAGESTAN, the `validator-committee` members process transactions in a **DAG** coming to consensus and finalising the transactions by adding them to the **Blockchain** thereafter. This is how DAGESTAN uses both the DAG and Blockchain architectures. DAGESTAN powers the finality gadget of Setheum, enabling near instant finality. However Setheum uses Substrate's BABE for block production, making Setheum natively a blockchain that leverages a DAG-based architecture for scalability and uses ***Cloud Proof of Stake (CPoS***), a custom type of Proof-of-Stake mechanism inspired by Polkadot's NPoS, as well as ***Cloud Proof of Work (CPoW)*** for Cloud Resource Proof. Nominators nominate Providers to be in the active set of chain Providers by staking their Setheum (SEE) with a Provider. Providers provide cloud resources in STEM Workers, produce new blocks, validate existing blocks, and also guarantee finality. Therefore, Setheum can use ***CPoS + CPoW*** to select Providers from a small set of the larger set of Providers, allowing even small token holders (***Nominators***) to nominate **Providers** who run infrastructure while still claiming staking rewards without running their own node infrastructure. And so with Setheum able to stay alive even when most of the network goes offline, Setheum COULD be able to survive WWIII.

Setheum EVM (Ethereum Virtual Machine)

The Setheum EVM (**SEVM**) enables Solidity smart contracts to be deployed on the Setheum blockchain with minimum changes. It also offers many distinct features such as "**multicurrency gas**" (paying fees in any tokens other than Setheum's native token), smart-contract access to All the built-in DeFi protocols and an **on-chain automatic scheduler** that enables use cases like subscription and recurring payments, **microgas** (paying very miniscule gas fees) etc.

FlexiFee: Network Gas Fee Mechanism

On-Chain transactions in Setheum can be paid in any token, not just in the PrimaryCurrency, any token can be enabled to pay for gas fees on the Setheum Network - both Mainchain and Subchains, this is called FlexiFee. The FlexiFee mechanism is facilitated by the Khalifa DEX, the token used to pay for gas is automatically swapped on the Khalifa DEX for the PrimaryCurrency used to settle the network fees payment. The fee paid is dissected into two (2), whereby 1:2 is moved to the Treasury and the remaining 1:2 is burned out of existence; this burn mechanism introduces a deflationary effect into the PrimaryCurrency which is the SEE.

STEM: Setheum Trusted Execution Machine

STEM Stack: Layer-2 Off-chain Computation TEE Enclaves

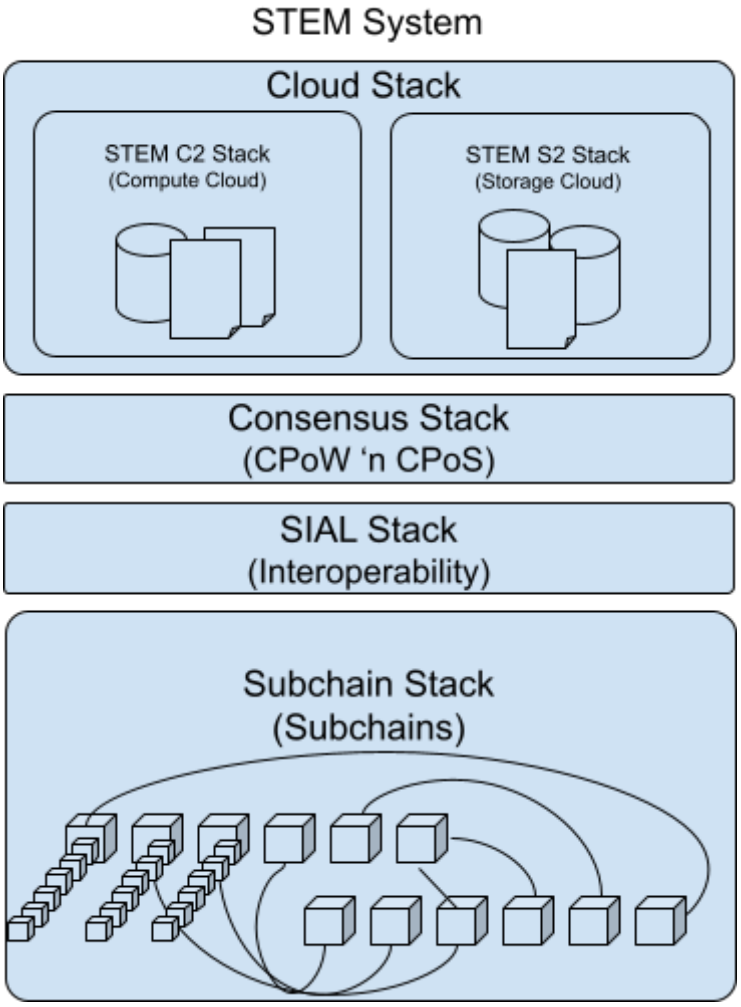

Fig-13: STEM Stack Abstraction

STEM System

The STEM(Setheum Trusted Execution Machine) System is one of the 5 Pillars of the Setheum Network, it is a fundamental core part of the network and is built to support TEE enclaves in the Setheum Network, making it possible to build multiple stacks of applications for the network such as the SIAL stack (`sial-stack`) built for interoperability, the `subchain-stack` to enable building of layer-2 blockchains (subchains), the Cloud Stack which comprises of the Compute Stack (`c2-stack`) and the Storage Stack (`s2-stack`), STEM also enables the `consensus-stack` which comprises of `cpow-consensus` and `cpos-consensus` that make the Setheum Cloud possible.

STEM Hardware Requirements for Running a Node in Setheum

Setheum uses a specific criteria of hardware that is planned to be expanded in the future. The hardware required has to support Intel-SGX as of now, and we have plans to later expand the hardware support to AMD SEV and RISC-V based TEE hardware. The hardware needs to have a confidence level of `tier-1`, `tier-2` or `tier-3` in order to be able to participate in Setheum either as a `provider`, `subchain-validator`, etc.

STEM Remote Attestation

STEM's Remote Attestation mechanism addresses the reliability issues related to code execution in TEEs(Trusted Execution Environments), and it is crucial in resisting potentially malicious behaviour. The `remote-attestation` protocol is a crucial part of the STEM system protocol, which is one of the pillars of the Setheum Network. Every `provider-node` needs to run through the `remote-attestation` process, it helps `verify` and `prove` the following 3 main objectives $_1$ Verify the identity of the node, $_2$ Prove the node's STEM Enclave logic has not been tampered with, $_3$ And Prove the node runs on supported required hardware with a genuine and untampered TEE.

Confidence Level Report

The STEM Confidence Level helps measure and score the safety of a STEM Enclave. It is generated from the `remote-attestation` report. The `confidence-level` helps notify and score a worker/node's security tier. There are 5 (five) Tier levels that are categorised and defined by certain parameters, such as `isEnclaveQuoteStatus` which indicates susceptibility to known vulnerabilities, and `advisoryIDs` which indicates the specific problem. Tiers 1, 2, and 3 are considered to be the best confidence level in security and thus acceptable because they are unaffected by any known vulnerabilities or the advisory is non-trivial. It is required to run nodes and workers that meet these tier levels. Tiers 4 and 5 are considered to be of reduced confidence level and thus reduced security because the node requires some BIOS or firmware configuration fix or the BIOS or microcode is `OUT-OF-DATE`. Therefore, since STEM only supports tiers 1, 2 and 3, providers with lower confidence level need to fix their issues in order to quality to run a node or worker on the Setheum Network.

STEM Data Sealing

The data sealing mechanism in STEM is to resist and defend cloud user data against sybil attacks and generation attacks. The STEM seals users' cloud storage data in its TEE enclaves, making it safe against these attacks such that even the nodes running STEM cannot actively generate sealed files from source files and data integrity is only verified on sealed files.

Cloud Proof of Work (CPoW)

Cloud Proof of Work is a consensus mechanism that uses compute and storage resources to provide cloud work for the network that will be used to quantify the proof of cloud work done by resources provided by the Provider(s). The CPoW mechanism involves subprotocols for quantification and QA such as the STEM Remote Attestation, Work Report, Data Sealing, Confidence Level Report, Proof of Empty Data Storage (PoEDS), Proof of Cloud Data Storage (PoCDS) and Incentivised Data Retrieval mechanisms.

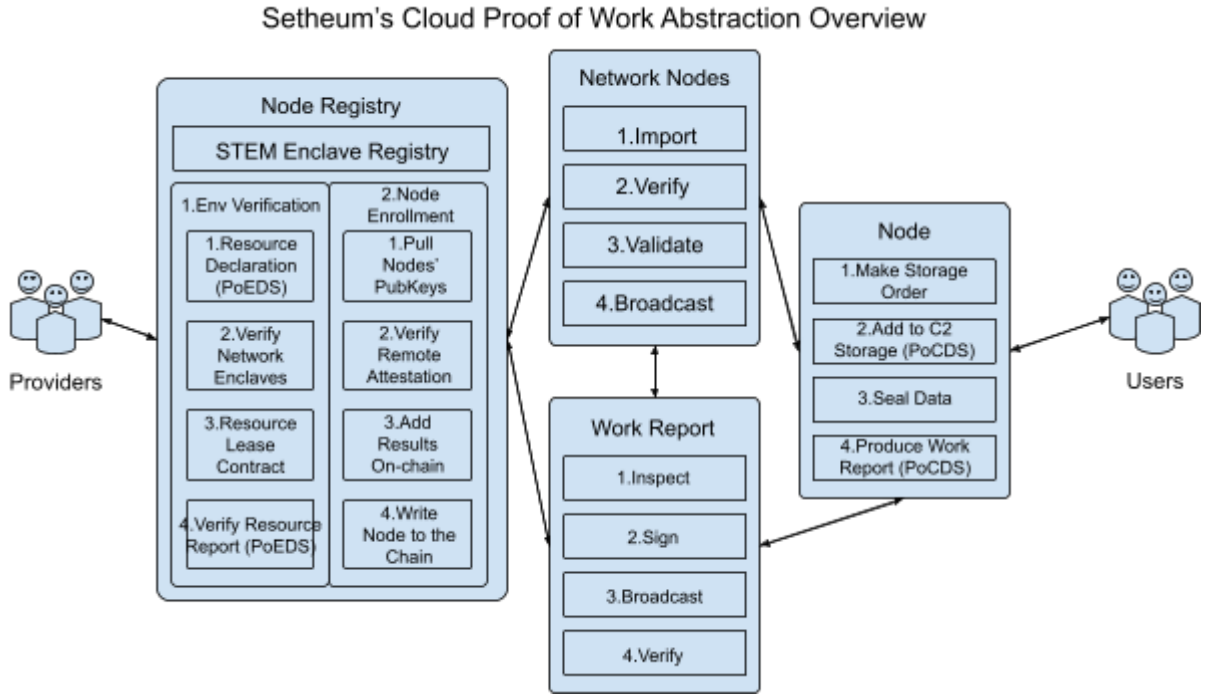

Fig-7: Abstract Overview of Setheum's CPoW (Cloud Proof of Work) mechanism

Proof of Empty Disk Storage (PoEDS)

This mechanism is used to measure and quantify the amount of Empty Storage Space a node provides, this works in the STEM enclaves in a trustless manner to efficiently verify the empty disk space declared/committed by the node, and STEM periodically undergoes this proof checks and verifications to ensure the validity of the available storage.

Proof of Cloud Data Storage (PoCDS)

The PoCDS mechanism in CPoW is in place to ensure the data integrity and reliability of cloud data storage on the network. This includes two main mechanisms for data integrity verification and for data space-time verification. Data integrity is verified via STEM's local TEE verification mechanism which includes data sealing and remote attestation while, data space-time is verified in a mechanism similar to the PoST (Proof of Space-Time) mechanism. CpoW's PoCDS greatly simplified the complexities of the PoST and PoRep mechanisms by leveraging STEM and its local TEE verification mechanisms.

Work Report

The Work Report mechanism of CPoW is meant to provide the proper examination of cloud workload of a node that runs CPoW, therefore, to ensure that cloud data are stored properly and completely, the CPoW node is set to periodically perform certain examinations on Merkle Hash fragments of stored cloud data and generate a storage declaration report in the STEM enclave where the report cannot be interrupted, altered or tampered with at the OS-Level, this gives the report the same hardware-level security as that of the TEE enclave.

Cloud Proof of Stake (CPoS)

The staking method in Setheum is a custom type of Proof of Stake mechanism inspired by NPoS(Nominated Proof of Stake), this mechanism advocates equality, randomness and fairness in the staking system in securing the network as well as earning staking rewards in the process. However the biggest difference between NPoS and CPoS is that in CPoS, the reliability of the Providers are tethered to the Cloud Compute Resources and Cloud Storage Resources (CPoW facilitated C2-S2 Resources) that account for the provider's voting weight in consensus and `StakingQuota`, the is a `StakingQuota` that each node is assigned relative to its proven cloud resources and work. CPoS uses the CPoW generated cloud work reports to measure the cloud resources that are set into the CPoS staking parameters.

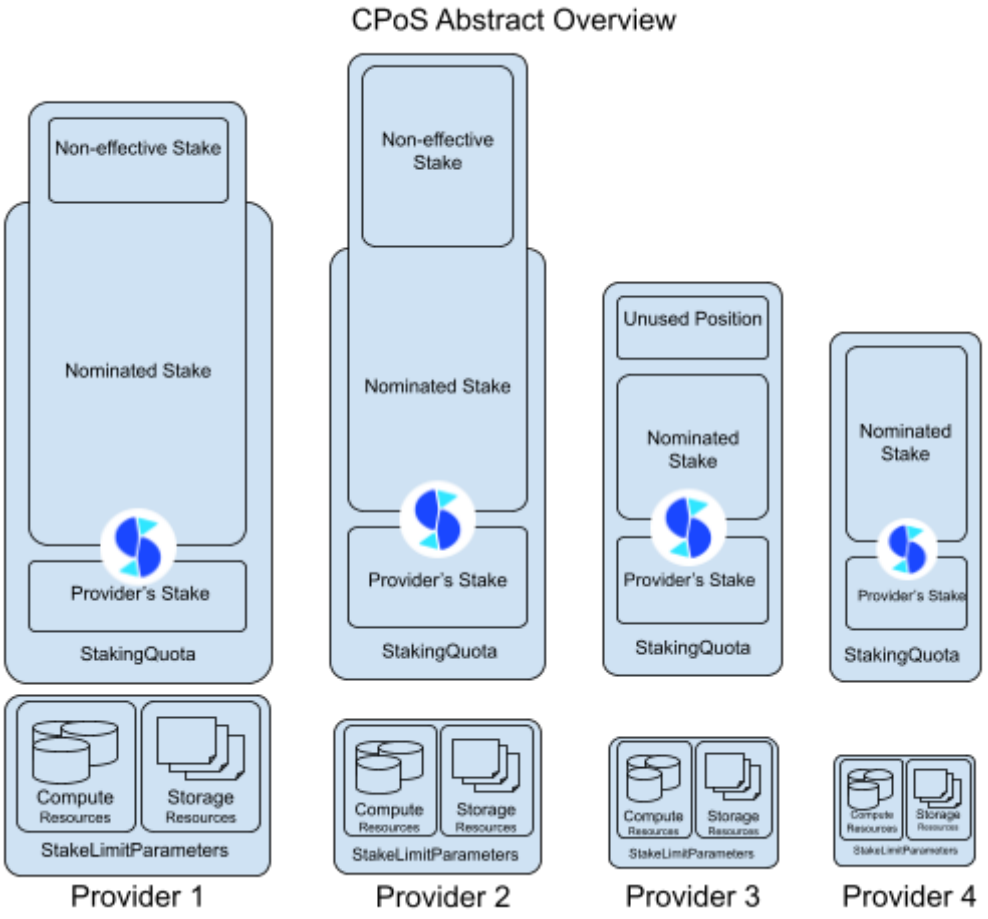

Fig-8: Abstract Overview of Setheum's CPoS

Providers earn SEE rewards to pay for their service as Providers that run and secure the network, nominators are also incentivised to stake their SEE to high quality provider nodes to earn staking rewards via nominations. This qualifies as Halal. All native protocols in Setheum are halal (permissible in Islam), they serve as the basis for a new internet, the decentralised internet (Web3).

Penalty and Slashing Mechanism in CPoS

Staked funds of unstable node providers or malicious nodes are slashed to incentivise stability, availability and reliability of nodes in the Setheum Network.The slashing mechanism is set in place to ensure reliability and availability of network participants such that the consensus verifiers are assured, protected and a penalty is given in the form of slashing to the concerned validator(s). The penalty includes slashing a portion of the validator's staked SEE tokens as well as removing the Verified identity Badge of the validator. The slashed amount is not burned right away but rather transferred to the network treasury, such that the slashed validator can appeal to get its funds returned within a certain period (ie. AppealPeriod), the slashed funds cannot be returned to the validator after the AppealPeriod has passed, thus staying in the Treasury. The formula for the SlashRatio is as follows:

$\chi = Min\{\frac{3 \times [\rho - (\frac{n}{10} + 1)]}{n}, 1\} \times 0.07$ where, n is the total amount of validator nodes, ρ is the amount of offline validator nodes, and χ is the SlashRatio.

Types of Staking Protocols in Setheum

There are two types of Staking protocols in Setheum, `StandardStaking` and `LiquidStaking`.

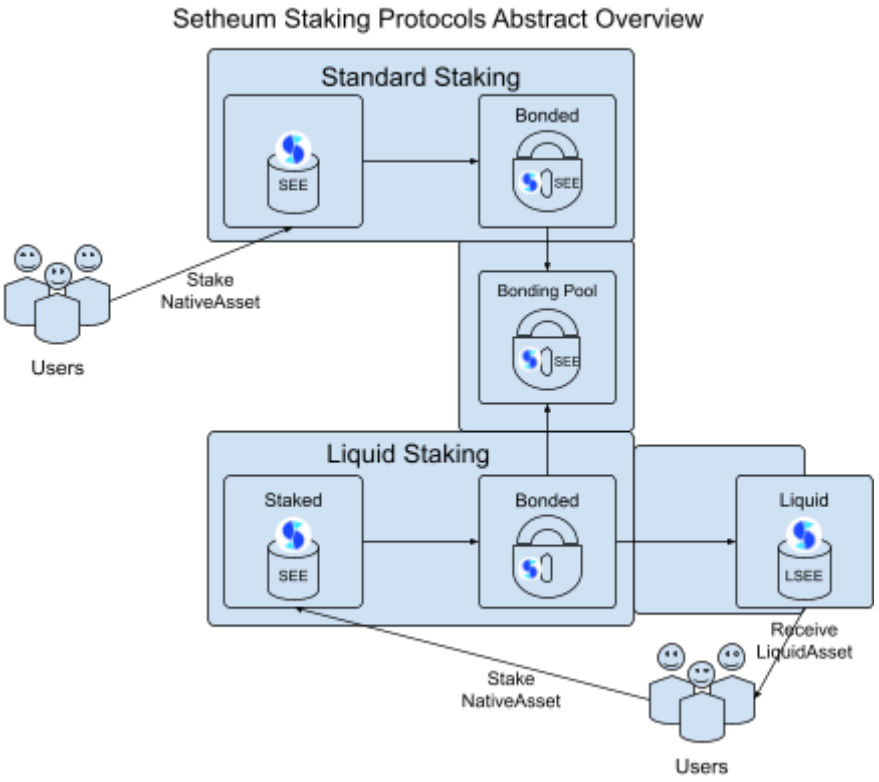

Fig-9: Setheum Staking Protocols Abstract Overview

Setheum Staking - Standard Staking vs Liquid Staking Comparison

✔️Criteria	Standard Staking	Liquid Staking
✔️Halal	✅	✅
✔️Native Protocol	✅	✅
✔️Main Staking Protocol	✅	❌
✔️Instant Unbond	❌	✅
✔️LSEE Liquid Asset	❌	✅
✔️Staking Rewards	✅	✅
✔️Stake SEE	✅	✅
✔️StakingQuota Allocation	✅	✅
✔️Slashing	✅	✅
✔️MultiProvider Nomination	✅	✅
✔️On-Chain	✅	✅
✔️Decentralised	✅	✅
✔️Permissionless	✅	✅

Fig-10: Setheum Staking Protocols Comparison Table (Standard Staking vs Liquid Staking)

Standard Staking in Setheum

In Setheum's Standard Staking protocol, stakers(providers/nominators) commit the `SEE` for staking on the network therefore securing the Setheum Network and earning `SEE` staking rewards in return. The `SEE` is the main staking token, however the `ComputeResources` and `StorageResources` determine a provider's `StakingQuota`. As more resources are committed, the system allocates more `StakingQuota` so that more staked `SEE` could be part of the `active-stake` that earns staking rewards.

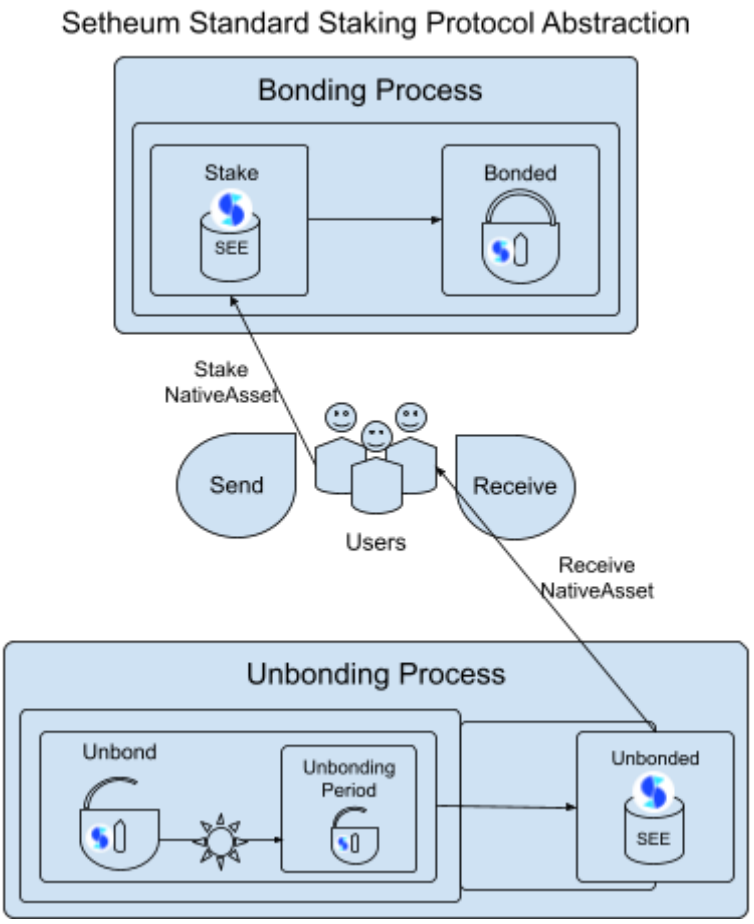

Fig-11: Setheum Standard Staking Protocol Abstract Overview

Liquid Staking in Setheum

Stake `SEE` while holding `LSEE (Liquid SEE)` for your market activity. When you stake a PoS chain's native currency, the token is locked in the system rendering it illiquid in order to secure the blockchain network. This is a very effective way to secure the network, however it is not efficient in terms of token economics, the more liquid the token is, the more efficient its market is. So what is the solution, here comes in Liquid Staking, as the name indicates, it is a way to stake tokens for securing the network while preserving the liquidity of the token in the market without compromising network security, but most liquid staking protocols out there are liable to compromising the security of the network, why, because they are not decentralised thus if they obtain the majority of the network tokens, these protocols can in fact be an attack vector for the network. In Ethereum 2.0 for example, the liquid staking protocol Lido finance makes for a good example of my point, it extremely centralises the network as we have seen that Lido finance controls over 1⁄3 of ETH staked in the network, and the ratio needed to be able to attack the network is 1⁄3, this makes the network prone to centralised attacks and censorship therefore making it more centralised. Setheum's liquid staking protocol solves that, it is a native built-in decentralised protocol built on Setheum's `DAGESTAN` consensus engine, but separate from DAGESTAN, using DAGESTAN as its backbone.

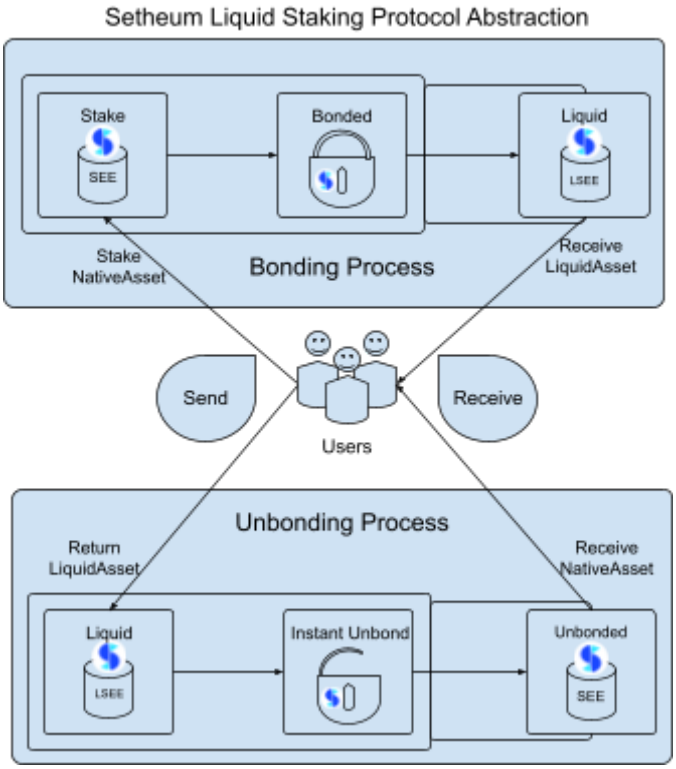

Fig-12: Setheum Liquid Staking Protocol Abstract Overview

Staking Rewards in Setheum

A definite amount of rewards are paid out per payout period, providers, nominators and the treasury are rewarded from that reward pool of 1 Billion SEE, 10%(100 Million SEE) to the treasury, 90%(900 Million SEE) to the Providers and Nominators. There is a minimum stake amount of 1,000 SEE for nominators, and Providers have a hardware requirement and a minimum stake of 250,000 SEE. A payout period is made up of 24 hour long eras made up of 96 sessions of 15 minutes each, nominators/Providers need to wait for the next era to initiate. The protocol allows any Setheum Provider to take part and allows nominators to choose which Providers they want to elect and stake with them.

Ethics of Staking in Setheum's CPoS

Setheum's ***Cloud Proof of Stake (CPoS)*** does not distribute block rewards to the so-called winning blocks or elite Providers that have the highest self-stake, it rather takes a lot of factors like nomination, CPoW, provider reliability, etc. into consideration to quantify a provider's score and `StakingQuota`. It is halal from my opinion and understanding and we say that it is Halal unless there is an evidence that it is haram from the Qur'an, Sunnah, Ijma' of the Sahaba or the Tabi'een, or the Atba' tabi'een, or ijma' of the Salaf AsSaliheen, or ijma' of the Ulama, or from the logical deduction according to the principles of the purposes of Shari'ah, and Allah knows best. The Ethical approach just happens to be the best option out there for best long-term economic sustainability and reliability with equanimity and equality of opportunities. Setheum just happens to implement just that for you and I.

Subchain Stack: Goodbye to MEV

Subchains are layer-2 blockchains connected to the Setheum Mainchain and secured by the STEM enclaves (Setheum Trusted Execution Machine) that are built on TEEs(Trusted Execution Environments) such as Intel-SGX , AMD-SEV, etc. with hardware-level security.

The Subchains layer provides computation confidentiality astronomical scalability with near instant subsecond finality and millions of TPS throughput, as well as cross-consensus interoperability with both STEM Stack Systems and Non-STEM Stack Systems via SIAL which also leverages STEM for trustless and permissionless cross-consensus interoperability. So we say goodbye to MEV on the Subchains Layer because it is confidential, this solves problems like front-running on Exchanges.

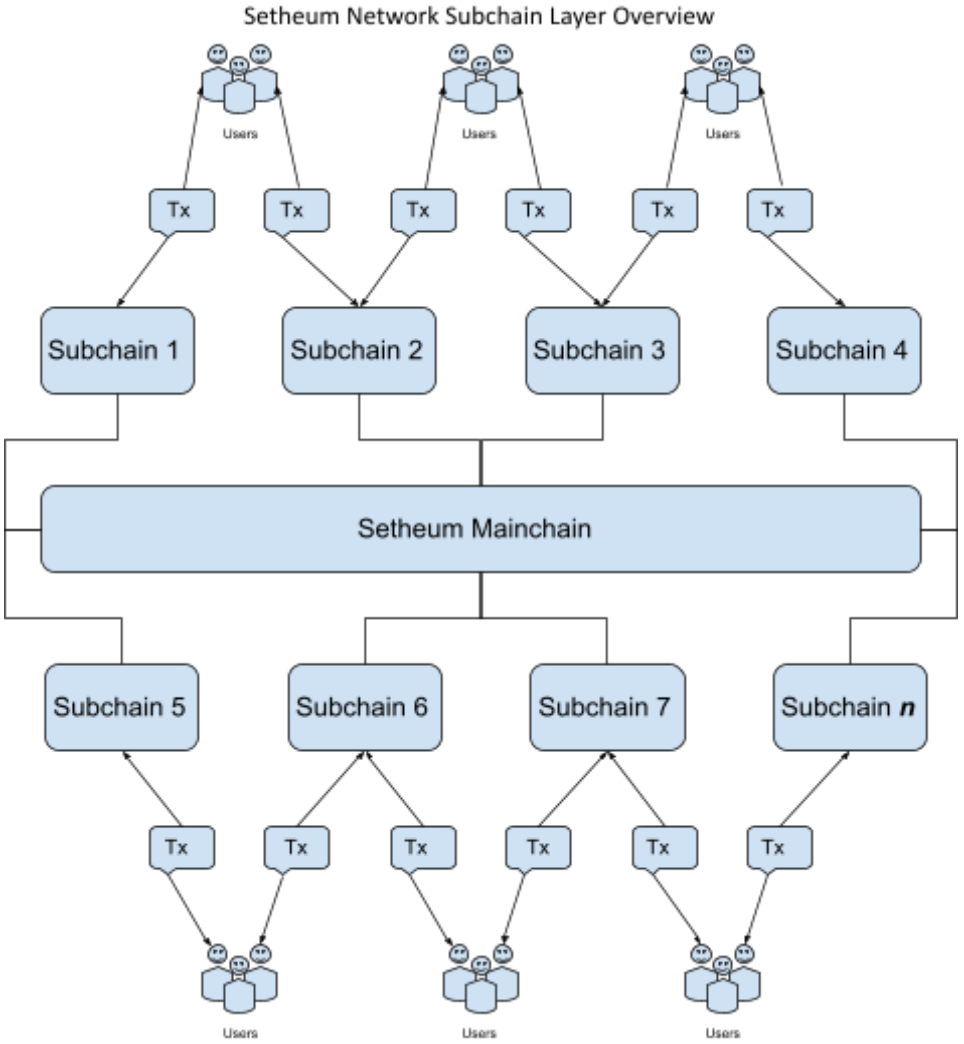

Fig-14: Setheum Network Subchain Layer Overview

We are building Setheum's first Subchain (Khalifa) as a DeFi Hub for the ecosystem, demonstrating the benefits of STEM for Subchains and DeFi applications like DEXs (with Khalifa Swap and many protocols on the Khalifa Exchange and many other DeFi protocols listed below in the Khalifa Subchain section.)

Setheum Cloud Stack: C2 and S2

Setheum Network provides a decentralised cloud compute and storage stack that makes the Decentralised Cloud Network accessible to everyone. The Setheum Cloud Stack consists of two main systems, the Simple Storage Cloud (S2) Stack and the Compute Cloud (C2) Stack. Setheum Cloud enables access to both decentralised storage cloud and decentralised Compute Cloud.

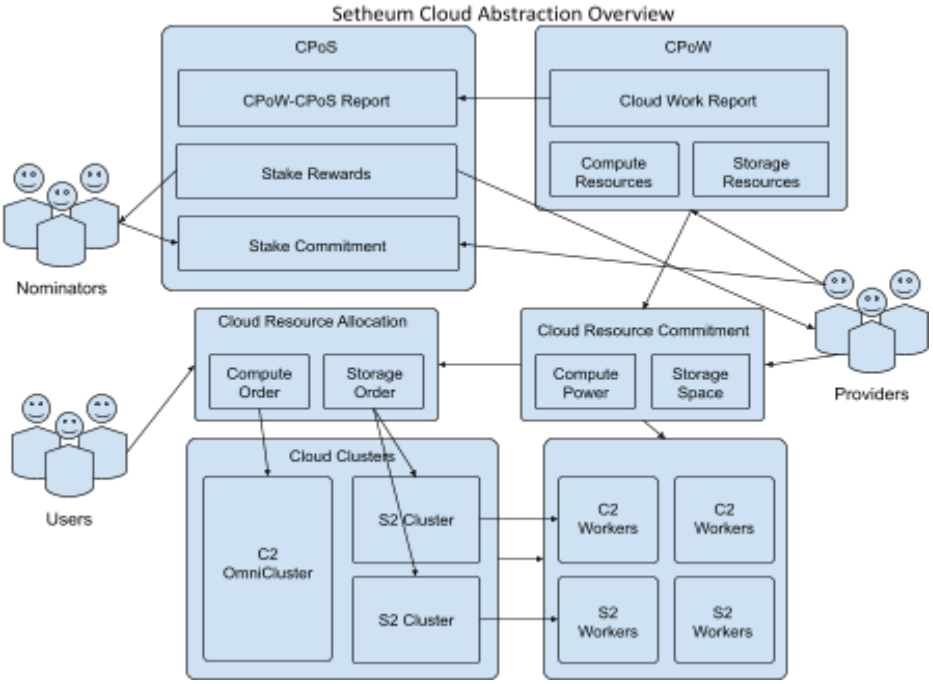

Fig-15: Setheum Cloud Abstraction Overview

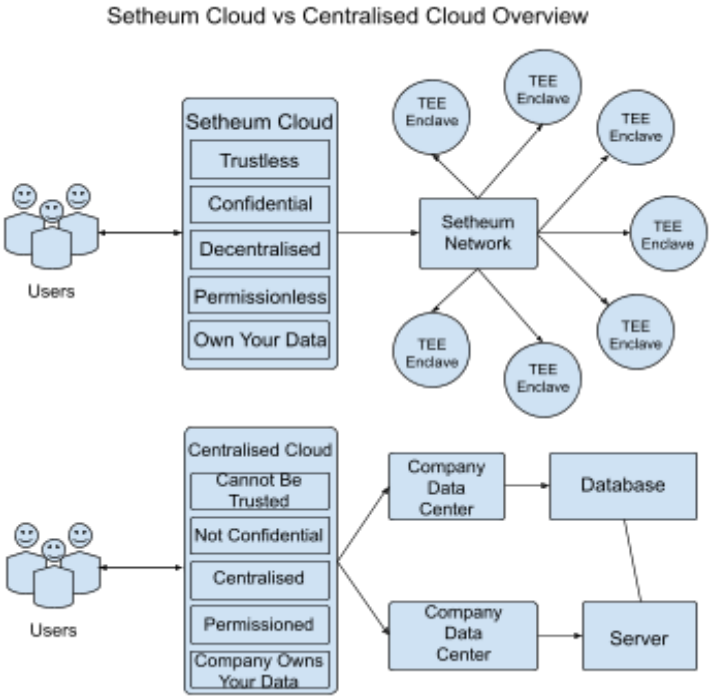

Fig-16: Overview of Setheum Decentralised Cloud vs Centralised Cloud

Setheum Decentralised Cloud vs Centralised Cloud Comparison

Criteria	Setheum Cloud	Centralised (AWS, iCloud, GCP, Azure, OVH, AliCloud, etc.)
✔️Trustless	✅	❌
✔️Blockchain Access	✅	❌
✔️Interoperability	✅	❌
✔️Scalability	✅	✅
✔️AI & ML Training	✅	✅
✔️Confidentiality	✅	❌
✔️Decentralised	✅	❌
✔️You Own Your Data	✅	❌
✔️Feeless Compute	✅	❌
✔️E2E Encryption	✅	❌
✔️App & Web Hosting	✅	✅
✔️ws/http Access	✅	✅
✔️Web3 Indexing	✅	❌
✔️Free Built-in Oracle	✅	❌
✔️Permissionless	✅	❌
✔️Secured STEM	✅	❌
✔️Accelerated Computing	✅	✅
✔️Storage Cloud	✅	✅
✔️Support Layer-2	✅	❌

Fig-17: Setheum Decentralised Cloud vs Centralised Cloud Comparison Table

Setheum Cloud vs Existing Web3 Decentralised Cloud Networks

Criteria	Setheum Cloud	IPFS/Filecoin	Crust	Phala	Arweave
✔️ Uses Proof of Stake	✅	❌	✅	✅	❌
✔️ Uses TEE Enclaves	✅	❌	✅	✅	❌
✔️ ws/http Internet Access	✅	❌	❌	✅	❌
✔️ Dedicated Storage Cloud	✅	✅	✅	❌	✅
✔️ Dedicated Compute Cloud	✅	❌	❌	✅	❌
✔️Dedicated Compute + Storage	✅	❌	❌	❌	❌
✔️ Accelerated Computing	✅	❌	❌	✅	❌
✔️ Free Built-in Oracle	✅	❌	❌	❌	❌
✔️ Support Layer-2 Subchains	✅	❌	❌	❌	❌
✔️ Off-Chain WASM Contracts	✅	❌	❌	✅	❌
✔️ Interoperability	✅	❌	✅	✅	❌
✔️ Feeless Compute Cloud	✅	❌	❌	✅	❌
✔️ `StakeToCompute` Model	✅	❌	❌	✅	❌
✔️ Stablecoin for Storage Order	✅	❌	❌	❌	❌
✔️ Stablecoin for Compute Order	✅	❌	❌	❌	❌
✔️ OmniCluster Cloud Compute	✅	❌	❌	❌	❌
✔️ Cloud App/Web Hosting	✅	✅	✅	✅	✅
✔️ Blockchain Node Deployment	✅	❌	❌	❌	❌
✔️ AI/ML & Metaverse Rendering	✅	❌	❌	✅	❌

Fig-18: Setheum Cloud vs Existing Web3 Decentralised Cloud Networks Comparison Table

Compute Cloud (C2 Stack)

STEM enables us to build the Setheum Network into a Compute Cloud Network, enabling confidential feeless off-chain computing with hardware-level security and also secured by Setheum's own DAGESTAN consensus engine's Staking mechanism, letting Providers provide computing and storage cloud resources to be able to participate in the operation of the network via ***Cloud Proof of Work (CPOW)*** and staking tokens as well as earning network staking rewards via our ***Cloud Proof of Stake (CPoS)*** where people who are not able to become providers can become nominators to back a number of Providers to take part in securing the network, providing Cloud Resources and earning staking rewards alongside their providers. Setheum's Compute Cloud (C2) is astronomically cheap to use because it runs on a feeless model where compute_calls are made off-chain on STEM and do not require consensus, therefore enabling us to provide a feeless Cloud Compute model. So, since it is feeless, we allocate computing resources to users based on a `StakeToComputeOrder` mechanism, where a user stakes SEE to get access to computing resources, the resources are allocated relative to the user's stake made where the allocation parameters are relative to the demand-supply curve of compute resources in the network. Setheum Compute Cloud enables a vast variety of applications to be hosted on the decentralised Cloud network, supporting application use cases such as AI and ML, Game and Metaverse Rendering, Accelerated Computing tasks, Trading Algorithms, On-Demand Scalable Applications, Supply Chain Applications, Industrial Design Computing, VPCs, VPNs, Serverless Applications, Websites, Servers, Databases, Data Analysis and Data Science, etc.

Compute Order

The `compute-order` mechanism in Setheum Cloud Compute (C2) is used to allocate compute resources from providers to cloud users. Th `ComputeOrder` mechanism enables users to make orders for Cloud Compute services to use compute resources of the network, which are allocated to them by C2's feeless `StakeToComputeOrder` algorithm which is responsible for allocating `ComputePower` relative to the user's percentage of stake in the `StakeToComputeOrderPool`.`Owning/Staking 1% of the StakeToComputeOrderPool` guarantees a `ComputePowerAllocation` of 1% of the `ComputePower` of the entire network.

C2 OmniCluster - Allocating Compute Resources in C2 Stack

The Setheum Cloud Compute (C2) OmniCluster mechanism is used to pool together all the cloud compute resources on the network in a single cluster that reliably aggregates computing power from all the provider nodes. The `OmniCluster` enables the c2 contracts running on it to communicate with each other, making them interoperable as in one execution environment, it provides reliability, and availability for c2 apps on it since the `OmniCluster` will provide compute resources to all the apps and contracts running on it even if most of the provider nodes go offline, and the resources are always allocated by the `ComputeOrder` mechanism.

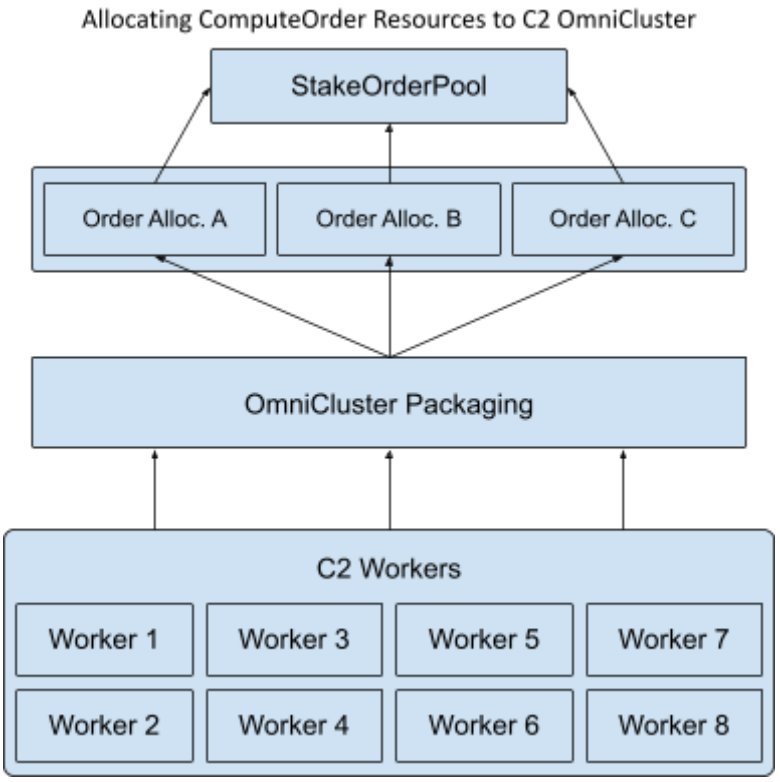

Fig-19: Allocating Compute Resources to C2 OmniCluster for Compute Orders in Setheum

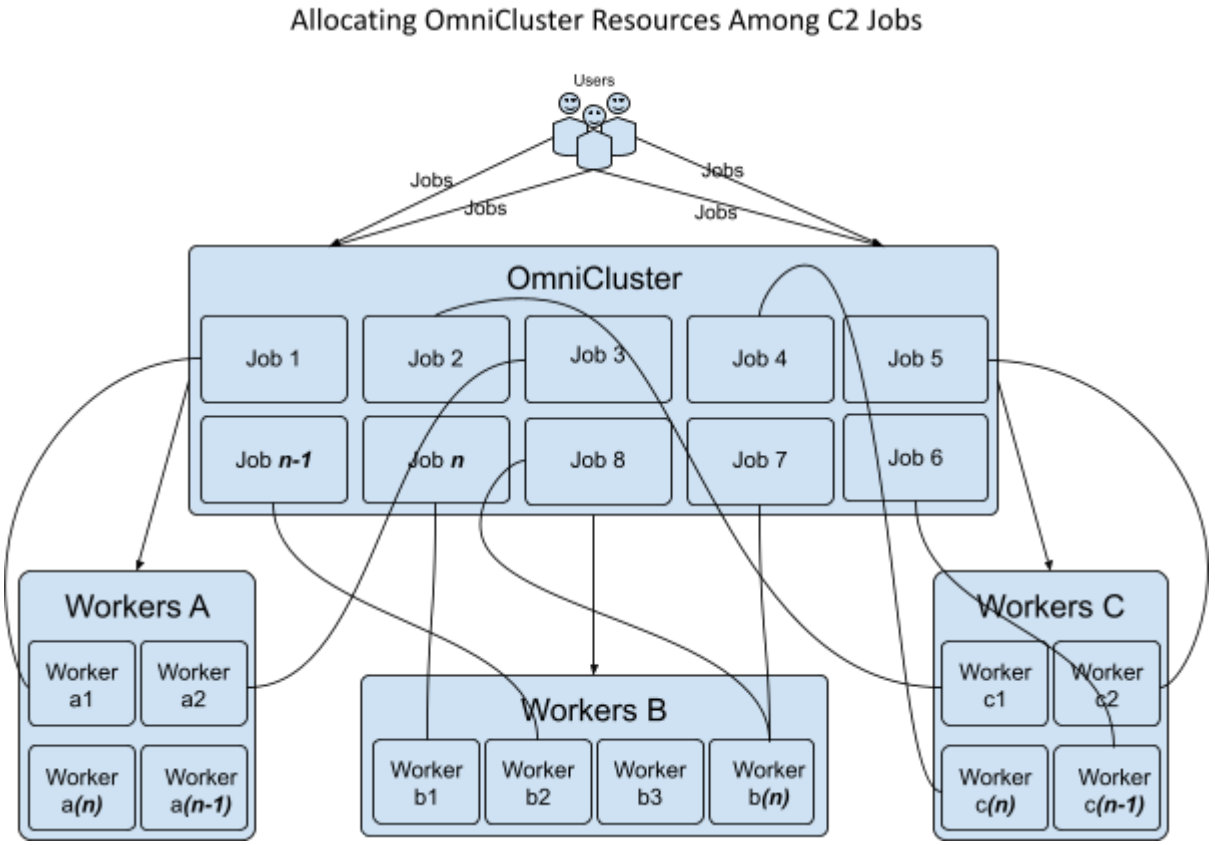

Fig-20: Allocating C2 OmniCluster Resources Amongst User Jobs in Setheum

Simple Storage (S2 Stack)

As STEM powers Setheum C2 (Compute Cloud), it also powers Setheum S2 (Simple Storage), where STEM builds a Decentralised Storage System into STEM to provide storage capacity and resources for the network users, as well as interoperability with Storage networks such as IPFS. App Developers can build fullstack apps on Setheum C2 where their database is stored on S2 integration, NFTs can be fully deployed at once on the Setheum Network where the CID addressed to S2 data, on-chain data could be stored off-chain on S2, games and metaverses could be built and rendered on C2 with their data stored on S2 without data compatibility issues, data migration hassles or external database problems, there are endless possibilities for the solutions this could enable. Setheum Cloud S2 Stack supports Metadata Storage Cloud, Website/App Hosting Cloud and Simple File Storage Cloud.

Storage Order

A `storage-order` in S2 is the mechanism used to allocate storage resources from providers to cloud users. The `storage-order` mechanism enables users to order cloud storage services to pay and store their files on the Setheum Cloud Network for the long term.
The user makes a storage order on the S2 Cloud at large and not to a specific node/provider in the network. The `storage-order` mechanism is pooled on the network whereby a pool of nodes store a file's replicas and the payment is also pooled and rewarded to the pool of nodes storing the user's file(s) replicas.

Data Retrieval S2 Stack

The S2 Stack provides both data storage and data retrieval services. It incentivises providers to provide efficient and reliable data retrieval services to cloud users for free, providers are incentivised with higher score to obtain data more effectively and thus increase its `StakingQuota` to earn more effective `StakingRewards` from the network's CPoS (Cloud Proof of Stake) consensus mechanism.

IPFS in S2 Stack

IPFS is integrated into Setheum Cloud such that a Setheum Cloud Node can retrieve users' cloud data through IPFS to the S2 Local Storage and also respond to retrieval requests of users or network nodes for exchanging data and data blocks. Nodes can obtain files through IPFS, storing them locally, then seal the data, and declare data storage on the Setheum Network, then provide verification and proof in local CPoW (Cloud Proof of Work).

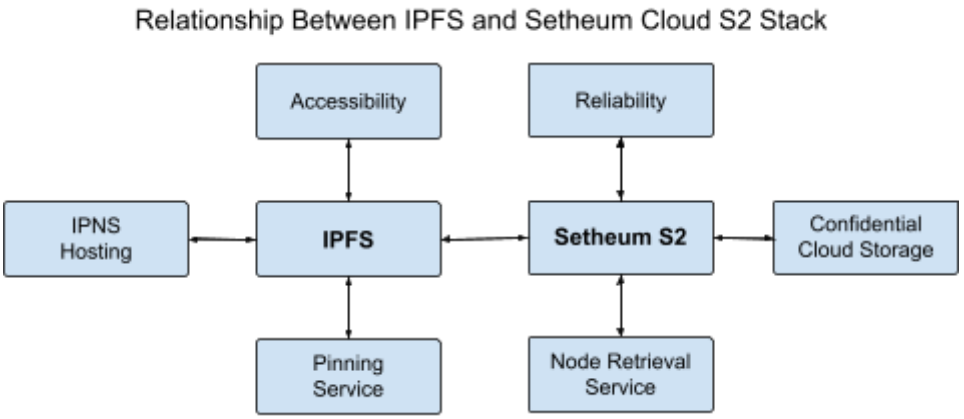

Fig-21: Relationship Between IPFS and Setheum Cloud S2 Stack

SIAL Stack: Open Interoperability

STEM enables SIAL (Setheum Interoperability Actuation Layer) to operate with hardware-level security, confidentiality, inherent interoperability and scalability. SIAL runs its OCWs(Off-Chain Workers) on STEM, these OCWs are secured by STEM and therefore do not need custodians for cross-chain swaps or trusted guardians for message passing relayers. SIAL-OCWs run light-clients and relayers on STEM as well as using STEM enclave invocations for cross-consensus interoperability. SIAL allows distinct consensus systems to directly communicate with each other, not just blockchains but also other systems like Oracles, APIs, Cloud Compute Clusters & Apps, etc, can communicate with all MultiLocations on SIAL.

SIAL: Setheum Interoperability Actuation Layer

SIAL is the Interoperability actuation layer of the Setheum network. It is a protocol that lets blockchains communicate with each other, such as EVM compatible chains, substrate chains using XCM(Cross-Consensus Messaging) over XCMP(Cross-Chain Message Passing) such as Polkadot, its parachains, and solochains, SIAL also uses the Chainbridge framework. SIAL enables not just balance transfers but also arbitrary messaging between these chains, it also enables smart contracts on these chains to communicate and execute cross-chain transactions.

SIAL Protocols

SIAL is built on XCM (Cross-Consensus Messaging) and XCMP (Cross-Consensus Message Passing), SIAL-XCB (Cross-Chain Bridge, built on ChanBridge), SIAL-XCC (Cross-Consensus Claims, inspired by XCLAIM), and SIAL-XCA (Cross-Consensus Aggregation, which translates XCB and XCC into XCM and aggregates their locations into XCM MultiLocations), then SIAL-XCM brings them together and SialBridge enables direct communication between all SIAL-XCM MultiLocations, making it the most interoperable and composable cross-consensus system.

Below are a list of SIAL protocols and an overview on how they work;

- **XCA:** Cross-Consensus Aggregation translates XCB and XCC messages into XCM and aggregates their locations into XCM MultiLocations;
- **XCB:** Cross-Chain Bridge connects XCM to EVM-compatible chains;
- **XCC:** Cross-Consensus Claims connects XCM to non-EVM-compatible chains;
- **XCM:** Cross-Consensus Messaging sets a standard for XCA messages and enables MultiLocations;
- **SialBridge:** SialBridge enables MultiLocations (Consensus Systems talking to XCM) to directly communicate back-and-forth with each other;

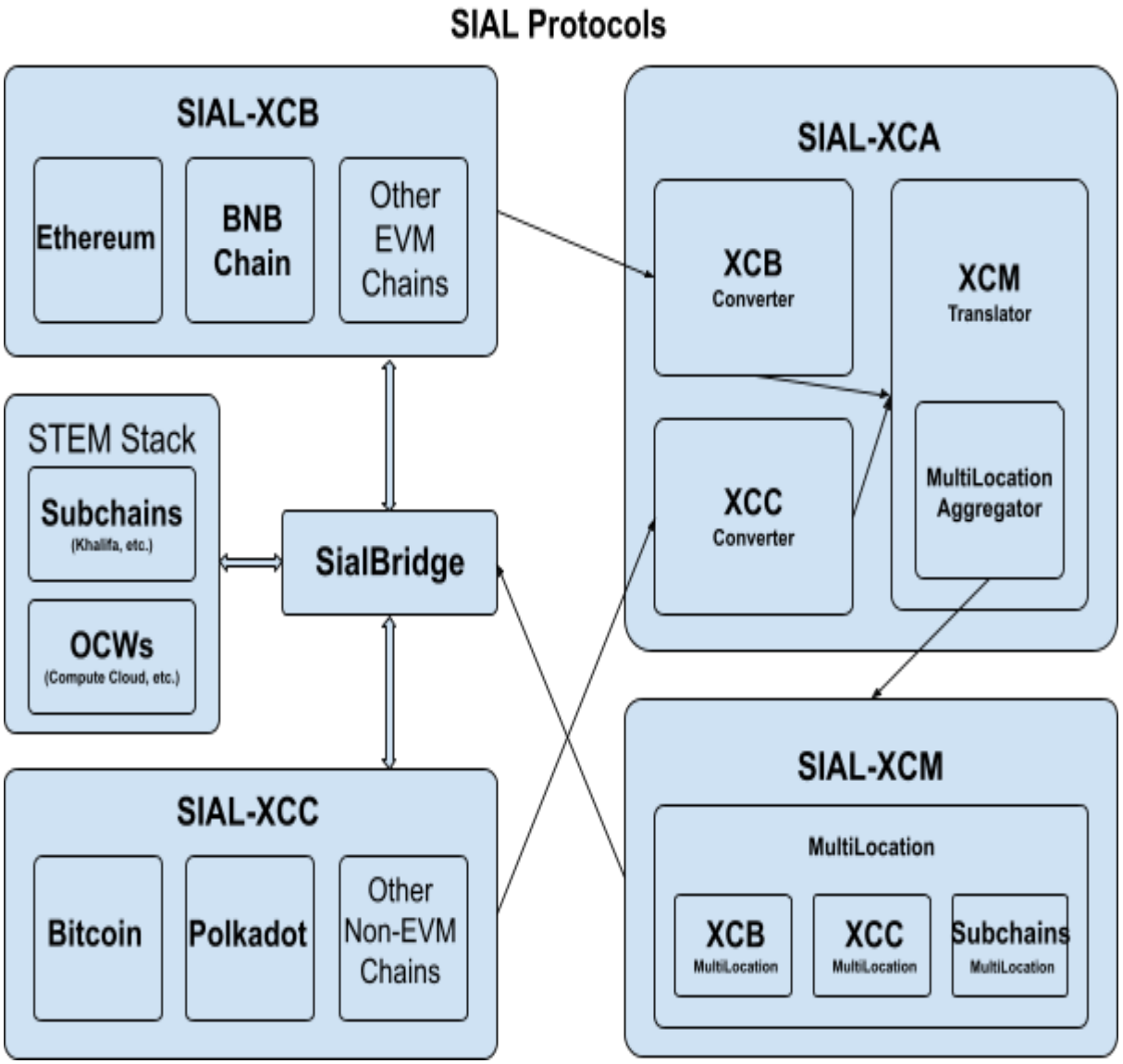

Fig-22: SIAL (Setheum Interoperability Actuation Layer) Protocols

Assets in Setheum

There are a variety of Asset types in Setheum, ranging from fungible assets to non-fungible assets, native assets to multi-currency assets and multilocation assets. This Asset classification and standardisation allows for diversity in letting specific use cases to be enabled and implemented on the network. Below are the asset types powered in Setheum;

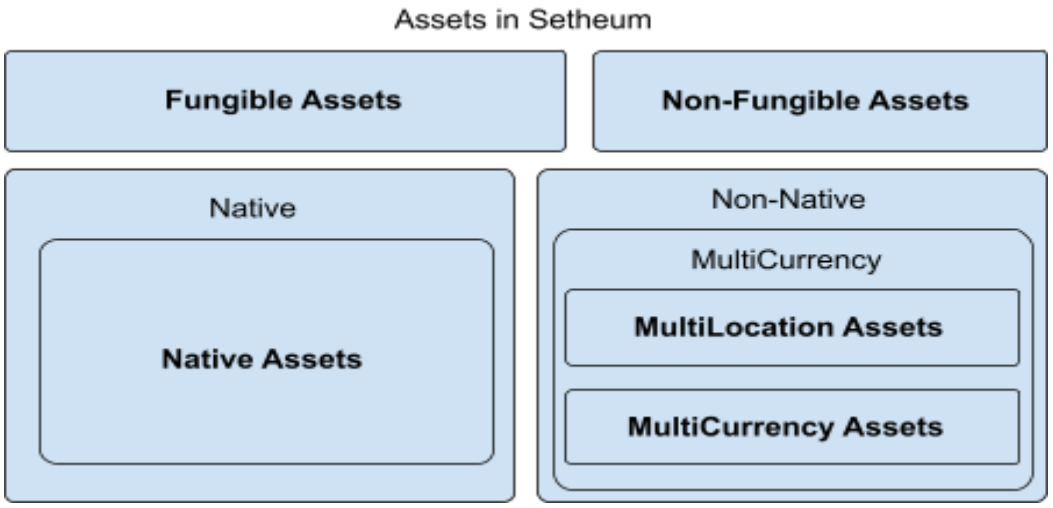

Fig-23: Overview of Assets in Setheum

- **Native Assets:** A blockchain's built-in assets (ie. primary-token/native-currency, SEE on the Mainchain, DOT on Polkadot, KHL on Khalifa Subchain).
- **MultiCurrency Assets:** Configurable non-primary non-native currencies (ie. stablecoins, multilocation assets, LP tokens, USSD, other assets).
- **MultiLocation Assets:** Cross-Chain Enabled Assets (ie. tokens from Subchains and other chains, KHL is a multilocation asset on the Mainchain).
- **Fungible Assets:** Assets that are interchangeable with one another (ie. ERC20, LP Tokens).
- **Non-Fungible Assets:** Assets that are not interchangeable with one another (ie. Digital Art, NFTs, Non-Fungible LP Tokens, Land Titles, Patents & other IPs)

Vesting in Setheum

Vesting is very important to be implemented, the initial issuance of tokens are to be vested for certain allocations to protect the community in general. There are various mechanisms and options in Setheum's vesting protocol that range from native vesting to smart contract vesting, cliff vesting to linear vesting, fungible and non-fungible token vesting etc. The parameters allow for three options regarding schedule types, cliff vesting, graded vesting, and linear vesting. LP tokens, ERC721 NFTs as well as ERC20s and various token standards covered by Sethem's MultiCurrency and MultiLocations Asset standards can be vested in the protocol.

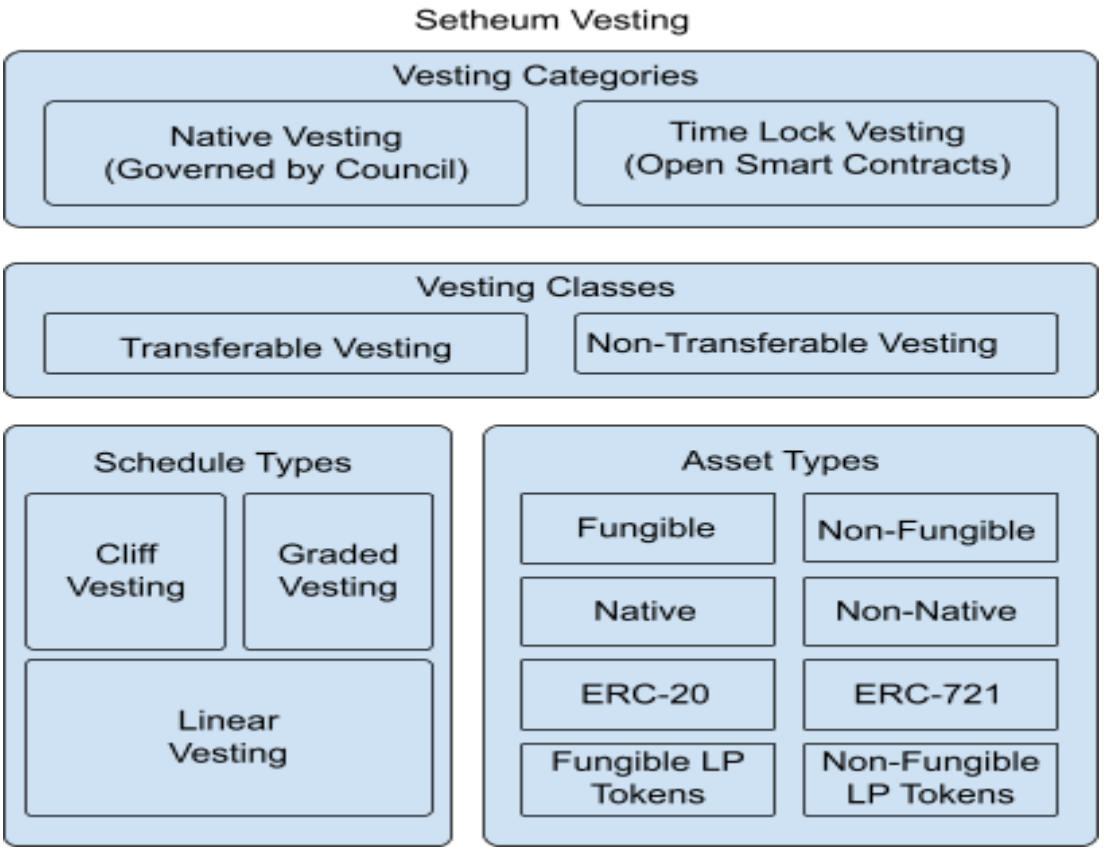

Fig-24: Overview of the Setheum Vesting Protocol

- **Native Vesting:** This category of vesting is carried out fully on the protocol's pallet and governed by the General Council;
- **Time Lock Vesting:** This category of vesting is carried out via the protocol's pallet and deployed as smart contracts, they are not upgradeable unlike native vesting. Anyone can deploy their own Time Lock Vesting Schedules.
- **Transferable Vesting:** This class of vesting allows for transferability of vesting schedules from one beneficiary to another. It is not in the form of tokens but replaces the `owner` with the `new_owner`.
- **Non-Transferrable Vesting:** This class of vesting does not allow for transferability of vesting schedules.
- **Cliff Vesting:** This type of schedule gets vested all at once at a specific timestamp (`vesting_period`).
- **Graded Vesting:** This type of schedule gets vested in grades of varying ratios over a specific period of time where tokens are vested in varying configurable ratios every `vesting_period`.
- **Linear Vesting:** This type of schedule gets vested gradually in a linear progressive over a specific period of time where tokens are vested in equal amounts every `vesting_period`.

Wallet Recovery in Setheum

We have seen a multiple of times when people or organisations lose access to their crypto assets either by forgetting their hardware wallet passcodes or losing its whereabouts, and many different other examples that go from the simplest of mistakes to very complex problems that all lead to losing access to valuable assets. Some people lose all their life's work to this class of problems, some lose all their savings, others lose all their investments or their hope and interest in this industry and seem to get confused worrying if this revolution has failed them or if they have failed it or both. A lot of us are guilty of this, many people went under and many people went extreme, but we are still here aren't we.This is why CEXs(centralised exchanges) have helped in onboarding most of the people coming into the industry and retaining most of them, CEXs can provide easy key management options and wallet recovery methods for their users. This is why CEXs also provide these custodial services not just to retail investors, family offices and newbies but also to institutional investors like banks, VCs and hedge funds. DeFi(Decentralised Finance) cannot reach mass adoption to the scale of centralised options without solving this class of problem, the wallet recovery problem. Thanks to the substrate framework and the talented team, contributors and ecosystem behind its development, we can now approach and ***solve the wallet recovery problem***. Setheum enables you to assign a list of contacts as wallet addresses to allow you to recover your wallet via these contacts ie. family, friends, colleagues. This is especially crucial when a person passes away for his/her family to be able to recover their wealth, or when a person loses his/her private keys thus cannot access their wealth, or even when an organisation loses access to their assets. Setheum provides the solutions for its users in all three scenarios.

- **Personal (Single) Wallet Recovery:** Could be a single wallet controlled by one signature.
- **Next of Kin (Federated) Wallet Recovery:** Could be a single wallet or a multiple of wallets controlled by a single proxy wallet. Could be recovered by a single signature contact/wallet or by a multisig wallet (controlled by a list of member signatures).
- **Organisational (Multisig) Wallet Recovery:** Or rather ***Multisig Wallet Recovery*** is a wallet controlled by a set of signatures/members all with their own accounts/addresses. Could be recovered by a single signature contact/wallet or by another multisig wallet (it is recommended to have it be controlled by a different list of member signatures/wallets that have different private keys from the ones used to control the wallet meant to be recovered, and ***avoid cyclic recovery to avoid losing chances of recovery***).

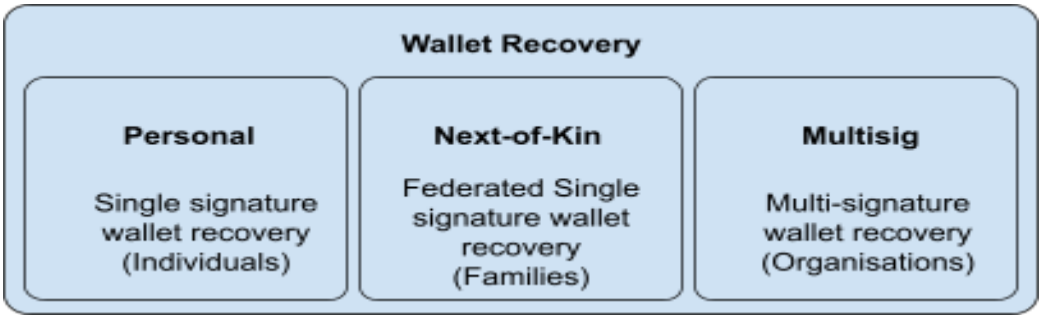

Fig-25: Wallet Recovery Overview

Personal (Single) Wallet Recovery

Setheum enables you to assign a list of close family members as next-of-kin to allow them to recover your wallet. This is especially crucial when a person loses his/her private keys/ seed phrase to be able to recover his/her wallet.

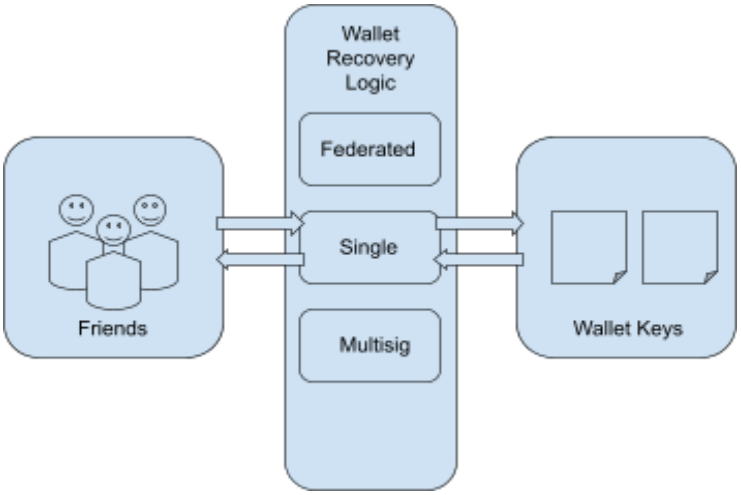

Fig-26: Single Wallet Recovery Overview

Next of Kin (Federated) Wallet Recovery

Setheum enables you to assign a list of close federation members as federated to allow them to recover your wallet. This is especially crucial when a person passes away for his/her family to be able to recover. Federated recovery setting lets each of the family members have weighted votes assigned to them such that one or more members can recover the wallet as a single signature or multisignature based on their weights in the federation. The weights have multiple parameters that can adapt to custom settings for how/who to recover the wallet.

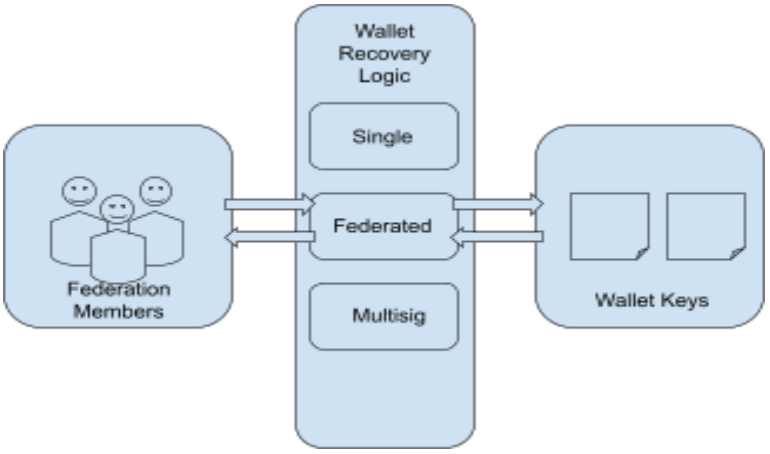

Fig-27: Federated Wallet Recovery Overview

Organisational (Multisig) Wallet Recovery

Setheum enables you to assign a list of multisig members as recovery options to allow them to recover a multisig wallet. This is especially crucial to recover an organisational wallet ie. belonging to a company or a DAO. A MultisigMember has to be a MultisigAddress.

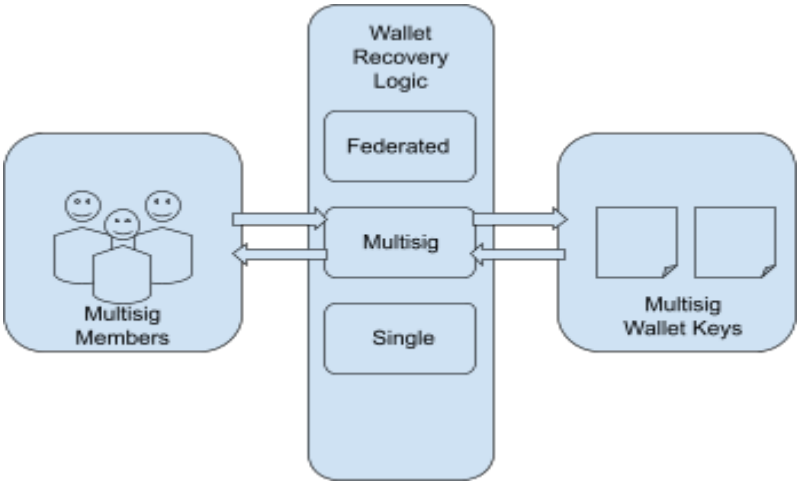

Fig-28: Multisig Wallet Recovery Overview

Khalifa Subchain - Setheum's DeFi Suite

This is Setheum's DeFi Hub and its first Subchain. Khalifa Subchain has the Khalifa Suite which is a platform of a suite of DeFi protocols powering Ethical DeFi solutions in the Setheum ecosystem. Khalifa Suite provides a range of protocols from a Liquid Staking protocol to Zero-Interest Stablecoins to a cross-chain DEX aggregator and Smart Liquidity Manager as listed:

1. **Liquid Staking:** Stake SEE/KHL while holding LSEE(Liquid SEE)/LKHL(Liquid KHL).
2. **Decentralised Zero-Interest Ethical CDP Stablecoins:** Shari'ah Compliant Zero-Interest over-collateralized Stablecoins backed by multicurrency *ECDPs*.
3. **ECDP Liquidation Pools:** Provide liquidity to liquidation pools to get access to assets during liquidations at liquidation premium and help keep a healthy ECDP system.
4. **Concentrated Liquidity AMM DEX:** Trade, farm yield and provide liquidity on Khalifa's *Automated Market Maker Decentralised Exchange*.
5. **Cross-Chain Swap DEX Aggregator:** Trade with best prices and cheapest fees with near instant finality on multiple cross-chain exchanges as one to enable cross-chain swaps via Khalifa's DEX aggregator between Setheum and other networks.
6. **Limit Orders on DEX:** Trade limit orders on Khalifa's *Automated Market Maker Decentralised Exchange*.
7. **Active Smart Liquidity Automated Market Maker (ASLAMM):** Provides a Smart Active Concentrated Liquidity protocol on the *Concentrated Liquidity AMM DEX* protocol in Khalifa.

8. **Liquidity Mining Incentives:** Mine Liquidity Incentives as an LP(Liquidity Provider) on Khalifa's *AMM DEX*.
9. **Time Lock Vesting Protocol:** Provides time locking and vesting for various types of tokens including native assets, ERC20s, NFTs, NFT LP tokens, and fungible LP tokens (for ASLAMM Liquidity Mining). This protocol supports time locking of assets as well as asset vesting schedules. The time locks and vesting schedules are deployed on the SEVM as smart contracts and can be used by anyone. This protocol is very different from the "***native vesting protocol"*** that can only be used via on-chain governance and is limited to a certain threshold of vesting schedules, where the "***time lock vesting protocol"*** has no such limitations.
10. **Khalifa TWAP Oracle:** Time Weighted Average Price Oracle for on-chain price feeds.
11. **Setheum Oracle:** An on-chain multi-oracle message system primarily for oracle price feed.

Chain Properties

Network	**Setheum**
Native Asset/Currency	SEE
EVM Chain ID	258
SIAL Chain ID	0
Primary Asset Initial Supply	10,000,000,000 (10B) SEE
Finality	1 Sec. (Subsecond for Subchains)
BlockTime	1 Sec. (Subsecond for Subchains)
MaxBlockSize	5 MB
BlockHashCount	2,400 (40 Mins.)
Session	900 (15 Mins.)
Era	96 Sessions (24 Hrs.)
Annual Inflation	1 Billion SEE
Min. Validator And Provider Bond	250,000 SEE (to be lowered as we grow)
Min. Nominator Bond	1,000 SEE (to be lowered as we grow)

Fig-29: Setheum Chain Properties

On-Chain Governance

Governance is the way rules, norms and actions are structured, sustained, regulated and held accountable. Setheum has a multicameral governance system with several avenues/chambers to pass proposals. Decisions in Setheum are enacted on-chain and are autonomous & binding. Setheum and Khalifa each have various on-chain governance chambers. The primary chamber is “the General Council” also called the “Shura Council”, it comprises a set of accounts. There is a Technical Committee for deciding on technical governance (e.g. runtime upgrades), a Referendum Chamber for democracy to allow all native token holders to participate in governance.

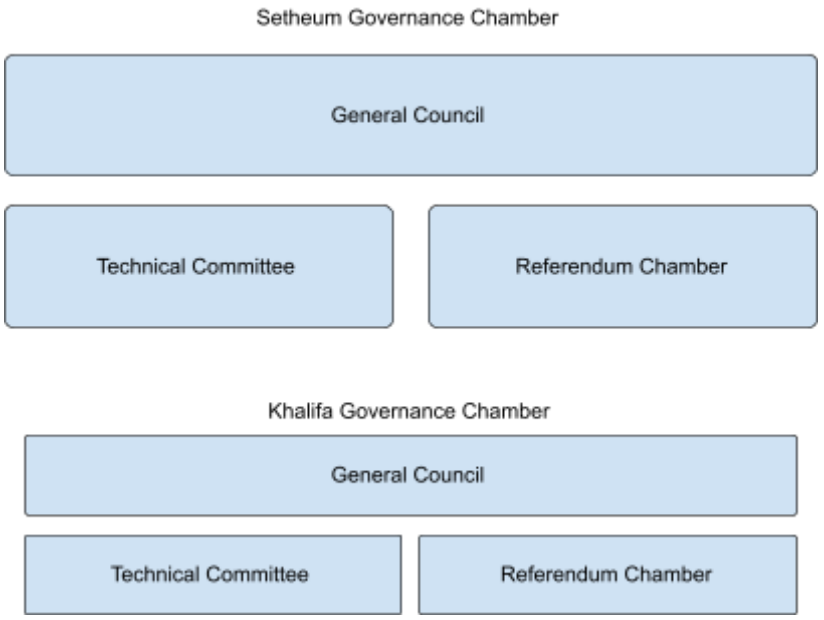

Fig-30: Setheum Governance Overview

1. **General Council:** General governance like approving runtime upgrades, it also elects Technical Committee members.
2. **Technical Committee:** They will be the **Committee** in charge of the governance of the Technical aspects of the Network like bug fixes and maintaining open source projects for example. The **Committee Members** are elected by the General Council.
3. **Referendum Chamber:** Simply enables democracy to allow all native token holders to participate in governance by voting on referendums. It is basically a **DAO (Decentralised Autonomous Organisation)** that governs a set of parameters that are put in place by the General Council. The **Council** proposes an on-chain update on those `parameters` then the **Chamber** votes on the proposal(s). Native token holders can also submit proposals to the **General Council**, the proposal is then voted on by the **Council Members**, if the proposal passes then it is forwarded to the **Referendum Chamber** as a public referendum to be voted on by the native token holders. The proposals are restricted to the `GovernanceParameters` of the **DAO/Chamber**.

Development Milestones

Launching of the Setheum Network will take a Phased approach, with **Damascus Testnet** launching in the **Phase-0, Setheum Mainchain Genesis** launching in the **Phase-1** with core modules, and the **Khalifa Subchain** launching in the **Phase-2.**

Setheum GitHub Repo Milestones Link: https://github.com/Setheum-Labs/Setheum/milestones

- [x] ~~Architecture - Infrastructure Research and Design~~
- [x] ~~Architecture - Token Economics Research and Design~~
- [x] ~~Architecture -Whitepaper~~
- [x] ~~Project Website Development~~
- [x] ~~Project Documentation~~
- [x] ~~Initiate Community Social Media Accounts~~
- [x] ~~Setup the Infrastructure~~
- [x] ~~Build and test the Blockchain (Devnet)~~
- [x] ~~Build Multi-Currency Native Support~~
- [x] ~~Build native built in DEX Protocol~~
- [x] ~~Build multi-currency flexible gas fee support~~
- [x] ~~Build CDP Stablecoin Protocol~~
- [x] ~~SEVM - Build SetEVM, an EVM layer for smart contracts~~
- [x] ~~SEVM - Precompiles and Predeploy Contracts~~
- [x] ~~SEVM - Build Setters.JS APIs, SDKs & developer libraries for EVM~~
- [x] ~~Build native support for NFTs~~
- [x] ~~Build Setheum.JS APIs, SDKs & developer libraries~~
- [x] ~~Liquidity Mining Incentive Protocol~~
- [x] ~~Build Launchpad Crowdsales MVP~~
- [x] ~~Khalifa Stablecoins - Update CDP protocol to ECDP protocol~~
- [x] ~~Khalifa Stablecoins - Pegged ECDP protocol~~
- [x] ~~Native Vesting Protocol~~
- [ ] Build STEM
- [ ] Build Subchain StackConsensus - Build DAGESTAN Consensus Engine
- [ ] Consensus - Build CPoW
- [ ] Consensus - Build CPoS
- [ ] Cross-Consensus - Build SIAL Protocol
- [ ] Cloud - Build Cloud-Stack (C2)
- [ ] Cloud - Build Cloud-Stack (S2)
- [ ] Staking - Build Staking Protocols (Standard Staking)

- [ ] Staking - Build Staking Protocols (Liquid Staking)Build the Khalifa Subchain
- [ ] Setheum Wallet Recovery protocol
- [ ] Oracles - Setheum Oracle (On-Chain Multi-Oracle Consortium)
- [ ] Update EVM to post London
- [ ] Update Setters-JS and merge it into Setheum-JS
- [ ] Launch Airdrop Event
- [ ] Launch Partnership Program
- [ ] Launch Bug Bounty Program
- [ ] Launch Ambassador Program
- [ ] Fundraising Rounds
- [ ] Phase-0 Launch **Damascus** Testnet
- [ ] Phase-1 Launch **Setheum** Mainnet
- [ ] Phase-2 Launch **Subchains**
- [ ] Enable Governance

Conclusion

Setheum has a unique approach to the problems facing the space and provides opportunities that incentivize adoption and usability and most importantly because it helps make Ethical Web3, Decentralised Cloud and DeFi available to anyone and everyone. Setheum has amazing investment opportunities with astonishing usability. Setheum is the brainchild of a cluster of ideas and challenges that inspire the founding of it. And so with the expected level of equilibrium, security, decentralisation, scalability, efficiency, diversity and adoption. Setheum via its Khalifa subchain, is set to implement the neom of finance in the Web3 Ecosystem extending hands to the halal consumer market and the Islamic Finance and Ethical Finance community by developing a wide range of Islamically permissible Web3 and DeFi products and services on the Setheum Network such as SlickUSD(USSD) and Setter(SETR) which is a zero-interest ECDP based crypto-collateralised stablecoin protocols, Khalifa also provides an Ethereum compatible smart-contracts layer (EVM), an on-chain built-in Decentralised Exchange (DEX), Liquidity Incentives etc.

References and Further Reading

1. Muhammad-Jibril B.A. (Khalifa MBA), ***Khalifa Blockchain: An Ethical DeFi Optimised Layer-2 Blockchain Built on Setheum for DeFi Confidentiality, Interoperability and Scalability | Technical White Paper***, [online] Available: https://github.com/Setheum-Labs/Setheum-Labs-White-Papers/
2. S. Nakamoto, *Bitcoin: A peer-to-peer electronic cash system*, 2008, [online] Available: https://bitcoin.org/bitcoin.pdf.
3. V. Buterin, *On public and private blockchains*, 2015, [online] Available: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/.
4. Jack Fransham, Parity Substrate, Polkadot, What is Substrate?, July 09, 2018, <https://www.parity.io/blog/what-is-substrate>
5. Alfonso Cevallos, Overview of NPOS, <https://research.web3.foundation/en/latest/polkadot/NPoS/1.%20Overview.html>
6. Jack Fransham, Polkadot Network - Medium, Never Fork Again, Nov 28, 2018, <https://medium.com/polkadot-network/never-fork-again-438c5e985cd8>
7. Kaihua Qin, Arthur Gervais, An overview of blockchain scalability, interoperability and sustainability, Hochschule Luzern, Imperial College London, Liquidity Network, <https://www.eublockchainforum.eu/sites/default/files/research-paper/an_overview_of_blockchain_scalability_interoperability_and_sustainability.pdf>
8. Stephan Cummings, Altcoin Magazine, The Capital - Medium, The Four Blockchain Generations, Feb 2, 2019, <https://medium.com/the-capital/the-four-blockchain-generations-5627ef666f3b>
9. Ibrahim Abu Sammy, Is Proof of Stake like Riba?, Published in Jamaa, Medium Publication, <https://medium.com/ummati/is-proof-of-stake-like-riba-`f9ad17c391a6>
10. Crust, White Paper v1.9.9, November 2020, https://crust-data.oss-cn-shanghai.aliyuncs.com/crust-home/whitepapers/whitepaper_en.pdf
11. Integritee AG, Integritee Lightpaper, 2021, <612892db018a36f054100b4d_Integritee AG Lightpaper.pdf (webflow.com)>
12. Hang Yin, Shunfan Zhou, Jun Jiang, Phala Network: A Secure Decentralized Cloud Computing Network Based on Polkadot, March 7, 2022, <https://files.phala.network/phala-paper.pdf>