Shardeum Litepaper

Executive Summary

The demand for decentralized applications running on smart contract platforms is exploding since use cases like AMMs, DeFi, NFTs, and Games are bringing new users into the space who otherwise were not interested in just cryptocurrency. However, current smart contract platforms are lacking in either scalability or decentralization. A lack of scalability leads to slow processing of transactions and higher transaction fees resulting in a bad user experience. A lack of decentralization is not immediately felt as a bad experience, but puts all the users at risk of a black swan event should the lack of decentralization be exploited in the future. Shardeum is an Ethereum Virtual Machine (EVM) compatible, smart contract platform which is designed to linearly scale while maintaining true decentralization and solid security through the use of dynamic state sharding. Partitioning of the nodes in the network into smaller groups called shards divides the workload and allows for more parallel processing. It also allows the platform to scale horizontally by adding more nodes to increase throughput. A network with a larger number of nodes will also have a higher degree of decentralization. Shardeum also incorporates many unique features such as linear scaling, node rotation, load detection, and auto-scaling to deliver the best user experience and long term sustainability of any layer-one smart contract platform. The Shardeum project intends to incentivize ecosystem projects to build innovative new applications on the platform as well as port popular applications that have been built on other platforms. Ecosystem incentives will also be provided to develop layer-two solutions to further increase transaction throughput, as well as create decentralized bridges to allow transfer of assets between Shardeum and other networks.

Background

In 2015 the Ethereum network made it possible for the first time to create smart contracts on a decentralized network and set off a revolution. Many decentralized applications have been developed and the popularity of Ethereum has grown over the years. Currently the demand for transactions on this network have reached the maximum capacity of 20 transactions per second (TPS). This has led to the transaction fees rising from under 1 cent in 2015 to about $50 in 2022. Many applications which were feasible on Ethereum are no longer sustainable due to the high transaction fees.

Even though Ethereum has plans to increase the transaction capacity, making changes to a production network holding billions of dollars of assets is very difficult and slow. Ethereum 2.0 will use sharding as a layer one enhancement to increase data availability. Sharding divides the nodes in the network into smaller groups which process different sets of transactions and achieve parallel processing. As Vitalik Buterin the founder of Ethereum pointed out, sharding is the solution to the scalability trilemma. The scalability trilemma says that as a blockchain tries to achieve scalability, decentralization and security, it will only be able to attain any two of these. With security being an essential requirement, there will be a trade-off between scalability and decentralization. Sharding provides a way to achieve both scalability and decentralization while maintaining security.

New networks which provide the exact same or similar smart contract functionality as Ethereum have been developed to fill the demand left by Ethereum. Among these new smart contract platforms a majority of them have given up decentralization to achieve higher TPS. We intentionally use the term “higher TPS” instead of “higher scalability” here because these networks are not designed to scale, but rather just raises

the bar from Ethereum's 20 TPS to a higher max TPS. Typically this is about 500 TPS. Once any of these networks hits the max TPS limit, it will experience the same high gas fees and slow processing times as Ethereum. Some popular smart contract platforms in this category include: Binance Smart Chain, Solana, Terra, Avalanche, Polygon and Algorand to name a few. These platforms can only increase TPS if each node in the system is upgraded to have more compute, storage and bandwidth. This is referred to as vertical scaling.

One of the first smart contract platforms to attempt sharding was Zilliqa. All nodes in this platform stored the complete state and every transaction was received by every node. However, for the purpose of validating transactions the network was sharded into multiple partitions based on the address space of accounts. This is referred to as compute sharding because it divides the work of validating transactions which is usually compute intensive. But since every node still receives every transaction and updates the state of all accounts, the network bandwidth and storage operations still become a bottleneck. This platform is able to achieve a higher TPS than a system with no compute sharding, but is not truly scalable since the network and storage are not sharded.

A more scalable approach to meet the growing demand for decentralized applications is to have an interconnected system of multiple sub-chains or sidechains. Such an approach is being taken by platforms such as Polkadot, Cosmos and Cardano. This approach can be referred to as functional sharding, whereby decentralized applications that need to interact with one another can be launched on the same sidechain. Transactions between contracts on the same chain are easy and in the case of Polkadot each parachain can process a max of about 200 TPS. However, transactions between contracts on different chains are essentially impossible. Instead assets and messages are expected to be passed between chains to coordinate interactions. Even though the TPS of a sidechain may appear low compared to networks like Solana, the ability to have multiple side chains allows such platforms to scale and the total TPS across all side chains can surpass that of platforms using only vertical scaling.

The most general approach to sharding is to divide the address space of accounts into multiple fixed size regions called shards and nodes in the network are assigned to different shards. This is referred to as state sharding. Such an approach is being taken by platforms such as Near, Elrond, and Harmony. Although Ethereum originally planned to implement state sharding, the new approach shards only the data to increase accessibility. In a network with state sharding, transactions between contracts in the same shard are fast and easy while transactions across multiple shards are much slower, but not impossible. If a transaction needs to affect more than one shard, it needs to be executed consecutively in each shard. Because transactions are grouped into blocks and consensus is done at the block level, transactions that affect multiple shards risk the possibility of being confirmed in one shard, but getting rolled back in another shard. To prevent this and maintain atomic processing of transactions requires additional complexity (see section 3.6). Also transactions which affect multiple shards will require additional processing time proportional to the number of shards they affect. Even with these complexities sharding is still beneficial since the TPS of the whole network will increase proportional to the number of shards it has. But due to the static nature of the shards, many additional nodes need to join the network before a new shard can be created. To date no production network has actually shown splitting and merging of static shards. This is why we introduced Shardeum. With our novel approach we further overcome limitations implied by static shards.

Features of Shardeum

Shardeum is an EVM, smart contract platform which is designed to linearly scale by using dynamic state sharding. Although it can be categorized with other state sharding platforms like Harmony, Elrond and

Near, it has some unique features that set it apart from the rest. While most platforms group transactions into blocks and apply consensus at the block level, Shardeum does consensus on each transaction separately. This allows a transaction that affects multiple shards to be processed simultaneously by these shards rather than consecutively as with block level consensus. This not only reduces the time to process the transaction even if it affects multiple shards, but also ensures atomic processing. Transaction level consensus eliminates the complexities needed to ensure atomic processing which otherwise are needed by block level consensus platforms. Another unique feature of Shardeum is that it uses dynamic state sharding. Unlike static state sharding where all the nodes in a shard cover the same address range, dynamic state sharding requires each node to hold a different address range, but there is significant overlap between the addresses covered by nodes. Although dynamic sharding is more complex to implement than static sharding, it allows for true linear scaling. Each node added to the Shardeum network immediately helps to increase the TPS, whereas with static sharding the number of nodes that must join has to be at least the number of nodes defined as the minimum shard size before another shard can be created. Only when another shard is created does the network TPS increase in a stepwise way with static sharding.

The following comparison will be limited to other smart contract platforms that are also working on state sharding. Although there are many smart contract platforms, many of them are focused on solving scalability with a short term view of vertical scaling using a small number of very powerful computers rather than taking the more difficult long term approach of designing horizontal scaling into layer one. Although Ethereum originally planned to implement state sharding, the new approach shards only the data to increase accessibility and relies on layer two to increase TPS. Like Ethereum, Shardeum will be able to use layer two to elevate TPS further. However, Shardeum will achieve increased scalability with state sharding in layer one which Ethereum appears to be abandoning due to the complexities involved. There are currently three well known smart contract platforms that are working on state sharding: Near, Elrond, and Harmony.

Even though some of these networks have launched their mainnet they are still in development and have much work to be done:

- Near: 1 shard with 100 nodes in mainnet. Expecting to add more shards in the future.
- Harmony: 4 shards with 250 nodes each for 1000 nodes total in mainnet. All contracts are in one shard.
- Elrond: 3 shards and meta chain with 800 nodes in each for 3200 nodes total in mainnet.
- Shardeum: 10 shards minimum with 128 nodes in each for 1280 nodes total; expected mainnet in Q4 2022.

Although Shardeum is still in development, the Shardus technology used at the protocol level has been demonstrated to achieve linear scaling. In the Q3 2021 update event a network of 1000 nodes running on AWS t3.medium hardware was shown to reach 5000 TPS of signed coin transfer transactions across shards. The shard size was 20 nodes, so with 1000 total nodes the network had 50 dynamic shards. The shard size was kept small to allow for more shards and better demonstrate linear scaling. Auto-scaling was also demonstrated in an earlier update event with the network detecting the transaction load and growing by allowing more standby nodes to become active nodes as the TPS increased. Later when the load was removed, the network shrank back down by removing some of the active nodes. The following table gives a sense of how much 5000 TPS is:

	Bitcoin	Ethereum	Polygon	Binance SC	Nasdaq	Visa	Twitter	Emails	Google	Text	Whatsapp
Avg TPS	3	15	40	60	1,200	6,500	10,000	11,000	99,000	254,000	1,100,000

Peak TPS	4	20	120	180		30,000					

Harmony is the only platform that is EVM compatible and supports smart contract development in Solidity and Vyper. The other platforms use WASM and require programming in more complex languages like C++ and Rust. Shardeum will be EVM compatible and will support smart contract development in Solidity and Vyper. Providing developers with the same EVM compatible platforms makes Shardeum instantly available to them without any modification to code or contracts.

The block explorers for all of these platforms have an interface that is very different from the EtherScan.io interface which users have become accustomed to. This is mainly because sharded networks have to deal with multiple blockchains and need to define their own custom interface. Shardeum plans to use an explorer that has the same interface as EtherScan. This is possible because after consensus the transactions can be packaged into a single blockchain for post-processing and storage. Shardeum believes that we should focus on improving layer one scalability and decentralization and not try to innovate the smart contracting language, the virtual machine, the explorer and other user and developer facing components of the platform. This will be key in gaining developer and user adoption of Shardeum. The following table compares some of the important metrics of smart contract platforms that are using state sharding.

	Shardeum	**Harmony**	**Near**	**Elrond**
EVM Compatible	Yes	Yes	via Aurora	No (WASM)
SC Language	Solidity, Vyper	Solidity, Vyper	Rust	C, C++, C#, Rust
Explorer	EtherScan like	Custom	Custom	Custom
Tx Fees in $	Low	0.000001	0.00044	0.005
Txs per Second	1 per node (100k TPS @ 100k nodes)	2,000 per shard (8k TPS @ 4 shards)	10 per shard (100k TPS @ 10k shards)	5,000 per shard (15k TPS @ 3 shards)
Nodes per Shard	128	250	100	800
Latency	10 Sec always for EIP2930 txs	10 Sec per involved shard	10 Sec per involved shard	10 Sec per involved shard
Consensus Alg.	PoQ + PoS	FBFT	PBFT	SPoS
Consensus Level	Transaction	Block	Block	Block
Current Shards	NA	4 but contracts on 1	1 unsharded	3 + meta chain
Sharding Type	Dynamic	Static	Static	Static
Scaling Type	Linear TPS per node	Stepwise TPS per shard	Stepwise TPS per shard	Stepwise TPS per shard
Archive Nodes	Yes	No	No	No

From this comparison it is evident that Shardeum offers many unique features not found in other sharded networks. One important feature unique to Shardeum is the use of archive nodes to offload historical transaction data from validator nodes. This means the validator nodes only have to store the state data and

require much less time to join the network. This reduces the hardware requirements of running a validator, allows more regular users to run validators and increases the level of decentralization.

Guiding Principles

Shardeum will be an open, collaborative and community driven project by taking an approach that's not been tried by other blockchains until now. The project will be as open as possible when it comes to discussions, information, ideas, documents and just about anything. Shardeum does not view anyone as a competitor because our goal is to enable the global adoption of decentralized applications. And that means collaborating with the ecosystem. The project will look for ways to help every individual or group building on top of Shardeum. It will collaborate with anyone who is trying to achieve a similar goal of increasing crypto adoption. Shardeum's core belief is that community is supreme and to involve the community in key decisions. But, decisions are just part of being community driven. An even more important aspect is to reduce the delta of project information. Whenever there is any new information to be shared we'll share that with the community as early as possible.

Shardeum Coin

The Shardeum network will have a native coin called Shard with a ticker symbol of SHM. The coin will be mined by validator, archive and standby nodes as reward for providing resources to the network. The coin will be used for paying gas fees associated with executing transfer transactions as well as smart contract execution on the Shardeum network.
Max supply: 508 million SHM
Distribution:

- 51% Community - reward to nodes; validators, archive and standby servers
- 18% Sale - 3 month cliff then 2 years linear vesting
- 15% Team - 3 month cliff then 2 years linear vesting
- 11% Foundation - unlocked at Token Generation Event (TGE)
- 5% Ecosystem & Airdrops - unlocked at TGE

Governance

A Swiss based foundation will support the development of Shardeum. The law firm assisting with the foundation setup is highly experienced in the cryptocurrency space as they were involved with the foundation setup of many other prominent crypto projects including Ethereum and Cardano. The long term goal is to transition Shardeum into a DAO. Various forms of DAO governance are currently being experimented with by many DAO projects. In the future DAOs will become more mature and recognized as legal entities by more jurisdictions at which time a smooth transition of Shardeum from a foundation to DAO can be considered.

Roadmap

Although Shardeum was started in early 2022, Shardus, the protocol level technology being used in Shardeum has been in design and development since 2016. Shardus is a framework for creating linearly scalable distributed ledgers. Shardeum will obtain a public project license to the Shardus framework by allowing Shardus token holders to claim 1% of the max supply. Shardeum will also provide additional staff to Shardus to accelerate the development timeline. By using the Shardus framework and adding EVM and

smart contracting functionality at the application layer, Shardeum will be able to reach mainnet much faster than otherwise possible.

- Q2 2022 - Alphanet
- Q3 2022 - Betanet
- Q3/Q4 2023 - Mainnet

These are tentative timelines and subject to change based on the completion of coding, testing, and other relevant factors to ensure that we reach our goal optimally.

Team

The founding members of Shardeum are Nischal Shetty and Omar Syed. Shardeum team members also known as committers are distributed across the US, India and Myanmar.

- Nischal Shetty - is the Founder and CEO of WazirX, India's largest crypto exchange with over 10 million users. Nischal is a highly regarded entrepreneur with over a decade of experience building and scaling global products out of India. A software engineer by education, Nischal has also founded Crowdfire, a social media management web service with over 20 million users in the past. Nischal's previous successes have landed him on the Forbes '30 under 30' list. A passionate blockchain evangelist, Nischal has been active in the Indian crypto space since its inception. Nischal's mission has been to make crypto accessible to every Indian; he's also been advocating positive crypto regulation in India with his Twitter campaign #IndiaWantsCrypto for over 1000 days.
- Omar Syed - is a blockchain architect who organized the Shardus project in 2017 to build a linearly scalable blockchain. Over the past three decades, Omar has been involved with helping large organizations such as NASA, Yahoo, and Zynga build scalable, fault-tolerant, distributed systems. Omar holds a B.S. and M.S. from Case Western Reserve University with specialization in Artificial Intelligence. Omar was involved with several start-ups including the first matrimonial website and the first stock sentiment analysis website. Omar along with his son Aamir invented the strategy board game, Arimaa, and offered the Arimaa Challenge Prize to promote breakthrough research in AI. Omar's long-term vision is a world where everyone receives an unconditional basic income based on a stable cryptocurrency so that poverty and hunger are eliminated.

Future Directions

The initial focus for Shardeum is to build the most optimal layer one solution with sustainable low gas fees while providing the same developer and user interface as Ethereum. After launch of the mainnet the goal of Shardeum will be to grow the ecosystem as quickly as possible.

Though the ecosystem evolves at such a rapid pace that it is impossible to predict what the future holds, we expect the following 4 broad areas for decentralized applications on Shardeum, each of these closely dependent and working in sync with one another:

1. **Infrastructure:** These are applications which will be the building blocks for the ecosystem to thrive. Some of these applications will be built ground up, while others will be existing applications which will be compatible with Shardeum. Some infrastructure applications expected are:
    a. DeFi(Decentralized Finance)
    b. DEX(Decentralized Exchanges)
    c. Physical and digital marketplaces

d. DAO tooling

e. Layer 2 scaling

f. Ecosystem builders including bridges to many other chains

g. Analytics, fraud detection and security

i. Stablecoin platforms

j. Oracle networks

l. Decentralized storage

2. **<u>Community (Peer to Peer):</u>** These are community built and community driven initiatives. Some of these can end up being huge nation building initiatives, serving the most underserved sectors which no business or government served well till date. Some of these community driven initiatives can potentially achieve in a few years, what we have failed to achieve in decades. Some possible applications are:

    a. Education

    b. Environment: Sustainability and restoration

    c. Citizen science projects

    d. Play to earn and unconditional basic income

    e. Identity

    f. Organic farming

    g. Peer to peer physical and digital commerce

    h. Renewable energy markets

    i. Metaverse- Open source, gamified, 3D AR/VR web experience with independent economies

    j. Digital collectibles and fashion in the metaverse- most major fashion brands have already made a move with NFT communities

    k. News media and social media

    l. Animal welfare

3. **<u>Enterprises:</u>**

    a. Affordable healthcare

    b. Manufacturing

    c. Supply chain

d. Smart infrastructure

e. Automation

f. Artificial Intelligence

g. Aerospace

h. R&D

i. Telecommunications

4. **<u>Academia:</u>** In the collaborative age, we expect academic and research driven approaches to be more prominent than ever in coming up with solutions for both enterprises and communities. Expect extremely trivial topics such as employment, labor, wages, organizations and basics such as food, transportation, energy and water systems to be researched in light of the new technology available in hand and re-defined to lift the quality of life for all species on the planet.

Current Version: 2023.06.22
Previous Version: 2022.03.08
First Version: 2022.02.25