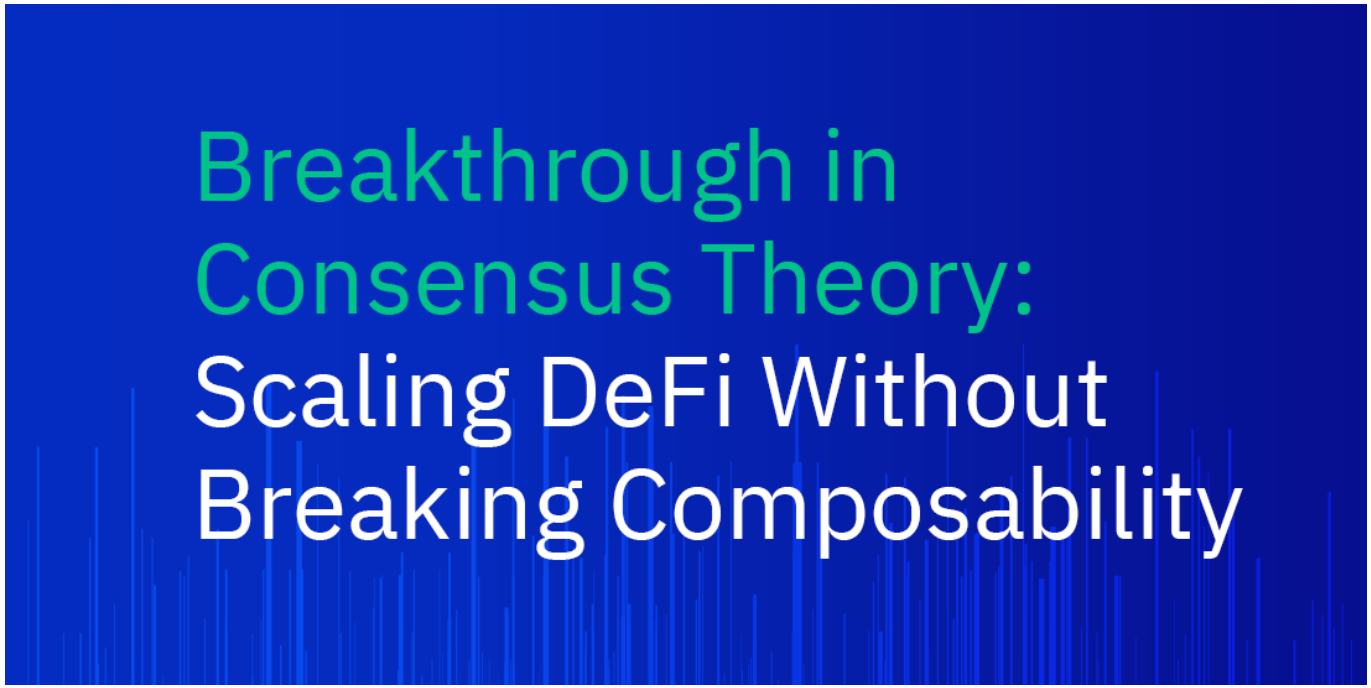
Breakthrough in Consensus Theory: Scaling DeFi Without Breaking Composability

Radix DLT — The Decentralized Finance Protocol Following
Aug 21 · 5 min read



Check out the recently published paper by University of California Davis' Prof. Sadoghi and his ExpoLab consensus experts that analyzed the inherent security and scalability of Cerberus' braided consensus design.

With Ethereum currently peaking at over $100 a transaction, it's clear that the world needs a better blockchain platform to take DeFi mainstream. That platform needs to fix the tech shortcomings holding DeFi back from broad adoption … while not *breaking* the stuff that has successfully taken DeFi to billions of dollars in locked assets (and counting) in a shockingly short period of time.

Top of the list of shortcomings is poor scalability, but the current solutions to this problem (simple forms of sharding and layer-2 solutions) fail the second part of the DeFi litmus test: they break composability, the most important tech enabler for DeFi there is.

Avoiding the compromises of Ethereum 2.0, Cosmos, Polkadot, and other "scalable" layer-1's, Radix and its breakthrough consensus design, Cerberus, uniquely provide the complete solution DeFi needs.

Now, the Cerberus concept has been formally proven in a groundbreaking paper written in collaboration between the Radix team and a consensus and

distributed systems Professor and his team of researchers at the University of California Davis. You can read that paper here: [link]

Scalability Matters, but Composability is King

Scalability is the key problem on the minds of those designing Ethereum 2.0 and a variety of new layer-1 DLTs coming to the market. For all of Ethereum's success as DeFi's dominant home today, transactions are extremely slow, unpredictable, and come with fees that would make a banker blush. These are the problems of poor scalability that kill DeFi's ability to compete with mainstream finance.

So how has DeFi gotten this far, despite Ethereum's inability to keep up?

A permissionless programmable DLT is the perfect laboratory for innovation around digital assets; a new way to make money using DeFi dApps on Ethereum is appearing every day — sometimes every hour. The wellspring of this innovation is a specific super power available to smart contracts on Ethereum today: **composability**.

Composability means that multiple dApps can be freely and frictionlessly combined. Composability makes it possible to build a DeFi service that, for

example, instantly provides the best exchange rate for a trade across multiple automated market makers, or allows the leveraging of a crowdsourced liquidity pool to take instant advantage of an arbitrage opportunity.

Crucially, to make these DeFi apps work, composability must be "atomic", meaning that either the entire transaction *across all of the dApps being composed* is valid and accepted all at once, or the entire transaction safely fails all at once. This (combined with decentralization) is what makes DeFi far more powerful, flexible, and open to innovation than traditional finance systems.

In short, no frictionless, atomic composability — no DeFi. But most DLT solutions seeking to increase scalability do so at the expense of breaking composability.

Most scalability concepts involve some type of sharding, whether using a hub-and-sidechain architecture (like Cosmos or Polkadot), by running a static set of blockchains in parallel (like Ethereum 2.0), or by breaking blocks into pieces for independent processing (like Near).

The problem with all of these is the same: different dApps and transactions are assigned to independent islands that make it impossible to conduct

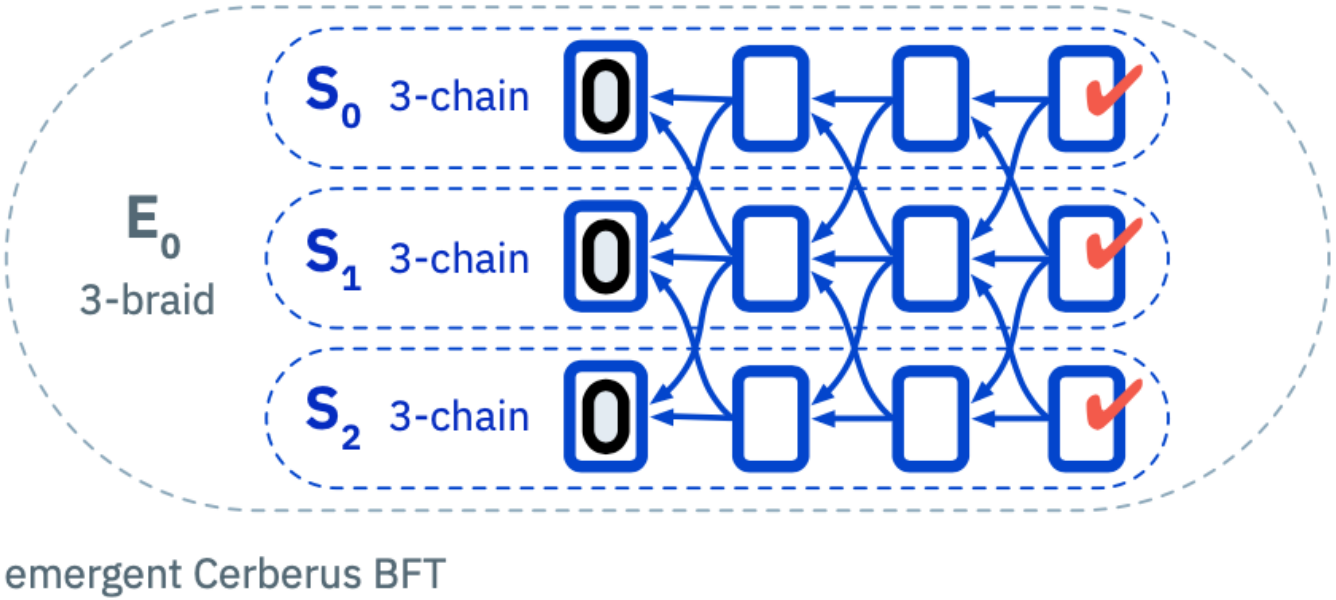
consensus for the entire transaction atomically. You can send messages in bottles between islands and try to coordinate between dApps in multiple steps, but that's far from the frictionless composability that makes DeFi work.

Cerberus: Sharding with Unlimited Scale and Composability

Radix has attacked this problem head-on with a new consensus design called Cerberus that is the end result of seven years of R&D. Cerberus introduces two significant changes from other scalable consensus protocols that give it practically unlimited scalability *without* compromising free atomic composability.

First, Cerberus uses a different kind of sharding. Rather than split dApps or assets between a static set of shards, Cerberus uses a practically infinite set of shards. Assets and dApps are represented *dynamically* across these shards. The result is limitless parallelism, meaning that no matter how much demand there is on the Radix network, natural financial incentives can just add more nodes to split up the load and increase throughput to keep up. This doesn't just raise the ceiling on scalability; **it means there is no ceiling**.

Second, Cerberus removes the barriers between its shards with a completely new consensus design. While each shard is able to conduct fast, secure consensus independently, Cerberus can directly "braid" these consensus processes together into one — atomically, and on-the-fly for each individual transaction. Braided cross-shard consensus is just as atomic and secure as simple single-shard consensus, meaning that **composability is just as free and frictionless as on a single blockchain, but without the scalability limits**. Cerberus gives Radix shards SpaceX satellite internet, rather than messages in bottles.



For each Radix transaction, Cerberus "braids" multiple single-shard BFT consensus (3-chains) together into a single "emergent" atomic consensus process (a 3-braid).

The upshot is that rather than fixing scalability by breaking composability, Cerberus delivers both without compromises.

We encourage you to read more about it in our Cerberus Whitepaper. But you don't have to take our word for it. We realize that solving the problem that so many others have not is a bold claim, so we've partnered with Prof. Mo Sadoghi's team of consensus and distributed system experts at University of California Davis to formally analyze and prove the inherent security and scalability of Cerberus' braided consensus design. You can view the results in a recently-published paper, now under peer review for the Journal of Parallel and Distributed Computing.

To learn more about how Radix technology solves the other problems holding back DeFi at every level, head over to our DeFi Whitepaper.

Composability Defi Radix Uc Davis Consensus