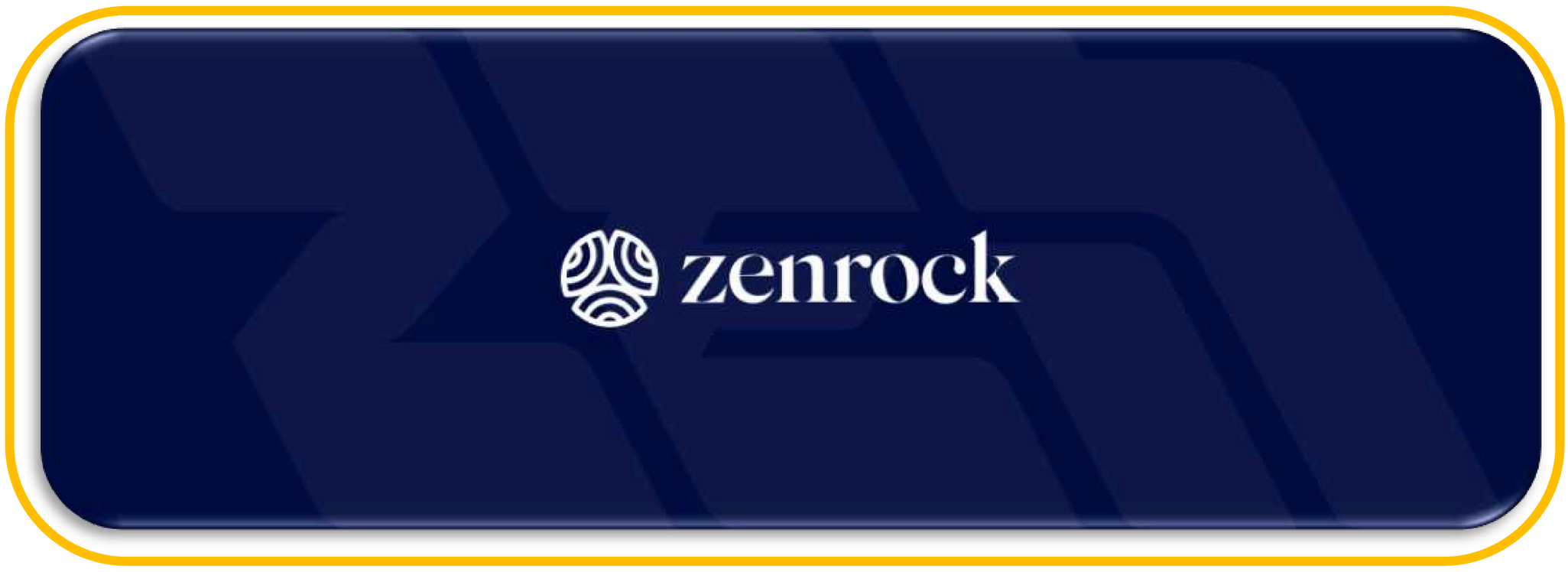
Zenrock, Decentralized Custody Standard, and the Future of Wrapped Assets



- ***Zenrock has developed a new custody standard for the onchain economy — built on crypto's most fundamental tool: the wallet.***

- ***Users keep control of their keys****. Unlike traditional wrapped assets, Zenrock uses Distributed Multi-Party Computation (dMPC) to deliver* ***custody without compromise*** *— users hold the keys, while the network secures the assets.*

- *Zenrock's* ***Decentralized Custody Token (DCT)*** *standard lets any project create secure wrapped assets backed by dMPC and* ***keep a piece of the economics****, turning what was once closed, custom, and permissioned infrastructure into an* ***open, standardized, and revenue-generating foundation.***

- ***zenBTC****, the first DCT, is a* ***wrapped Bitcoin designed specifically for Solana.*** *It is yield-bearing, fully decentralized, and has no single points of failure.*

- ***zrChain****, a purpose-built Layer 1 blockchain, serves as the neutral, transparent custody foundation that powers all DCTs.*

- ***$ROCK****, Zenrock's utility and governance token, is designed with* ***economics built-in from launch. No future fee switch or implicit trust required.***

The Need For a Custody Standard

Since DeFi Summer, crypto infrastructure has come a long way. Transaction fees have plummeted, blockchains have scaled, user interfaces have matured, and cross-chain messaging is on its way to becoming ubiquitous.

But one foundational piece of the puzzle is still lagging behind: **custody.**

In a multichain world, the ability to move assets securely across ecosystems is essential. Yet while solutions like LayerZero's OFT standard have advanced interoperability, they only go so far. L1 gas tokens like BTC, SOL, and ETH — arguably the most important collateral in the ecosystem — don't natively support these models.

That's where lock-and-mint remains indispensable. The concept is simple: lock the asset on one chain, mint a representation on another.

But conventional systems concentrate all assets in a single custody contract or vault — **creating massive honeypots and single points of failure due to concentration risk.**

Given this backdrop, the lock and mint mechanism has not reached its full potential. Not because the tooling doesn't exist, but because **users don't trust how it's implemented.**

And that is for good reason!

Locking and minting cross-chain mechanisms have been responsible for countless hacks and exploits onchain.

Zenrock's model is different. Custody is distributed across a network of Externally Owned Accounts (EOAs) powered by dMPC, there's no centralized vault to target or honeypot to drain.

It's **self-custody.**

Unlocking Crypto's Foundational Technology: The Wallet

At the heart of Zenrock's custody system is a simple but powerful tool: **Externally Owned Accounts (EOAs).**

An EOA is the most basic type of account on any blockchain — **a wallet** — simply a private key and a public address. **No smart contracts, no dependencies.** It's the lowest assumption, most universally proven infrastructure in all of crypto.

Zenrock leverages EOAs as the endpoint for all custody. Instead of holding a private key in one place, **zrChain shards the key using dMPC.** As a result, multiple independent parties hold fragments of the key and come together to generate signatures — **never exposing the full key at any point to any party — including Zenrock.** This design combines the simplicity and resilience of wallets with the security of threshold cryptography.

Critically, this approach avoids reliance on smart contracts or chain-specific logic. EOAs don't break when a chain upgrades. They don't depend on fragile hooks or protocols that might be deprecated. They just work — now, and in the future.

By anchoring custody to EOAs and running the entire custody layer on a purpose-built chain, **Zenrock keeps custody neutral, portable, and secure — no matter how destination chains change.**

Core developers cannot possibly look through every lock and mint mechanism on their chain before pushing an upgrade or altering a client, **but they will definitely make sure that wallets still work perfectly.** With DCTs that's all that matters.

Custody Without Custodians

At Zenrock, we don't custody your tokens — you do.

Using distributed MPC, users retain control over their keys while our infrastructure ensures assets are securely locked. It's **self-custody**, **enforced by dMPC technology rather than trust.**

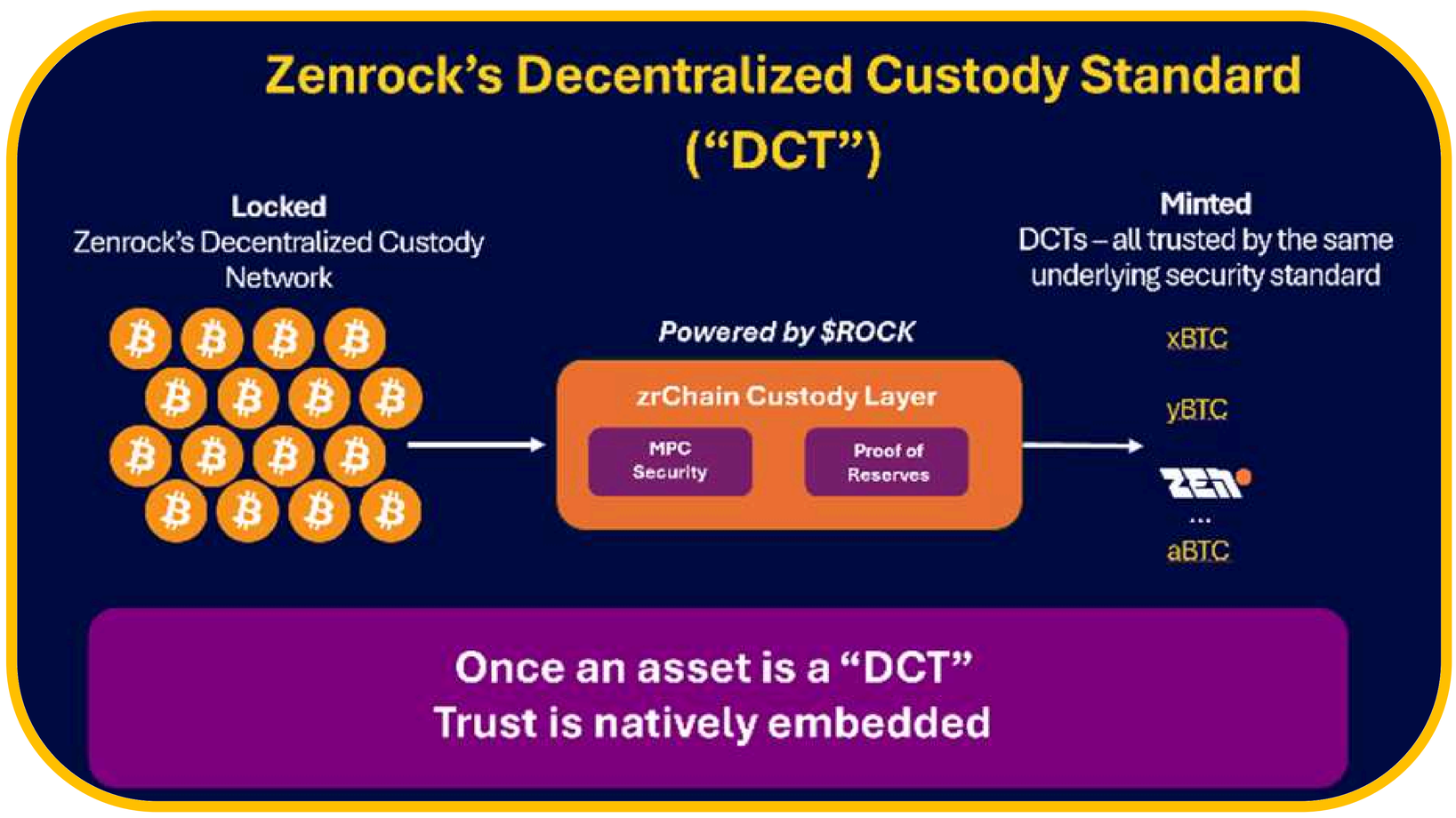
Not your keys, not your coins – isn't that the first thing we all learn in this space? Why would that not apply to the future of assets in the onchain economy?

Introducing the Decentralized Custody Token (DCT) Standard

At Zenrock, we're tackling this issue head-on with a new primitive: **Decentralized Custody Tokens ("DCTs").**

A DCT is any token issued through Zenrock's decentralized custody network. Secured by distributed multi-party computation (dMPC) and anchored by zrChain, **the DCT standard sets a new benchmark for trustless, onchain asset security.** It reimagines what custody can be: **resilient, transparent, self-custody that is always secure.**

With DCTs, developers can create secure, composable cross-chain representations of any asset — from Bitcoin to dogwifhat.



DCTs are much more than just 1:1 wrappers. **They're a security foundation.**

Many DeFi primitives can be built on top of a DCT — structured products, leveraged vaults, restaking strategies, point-optimized wrappers, even onchain perps. That flexibility is intentional. Developers can take creative risks. Users can choose their exposure.

But no matter what's built on top, the underlying custody stays the same.

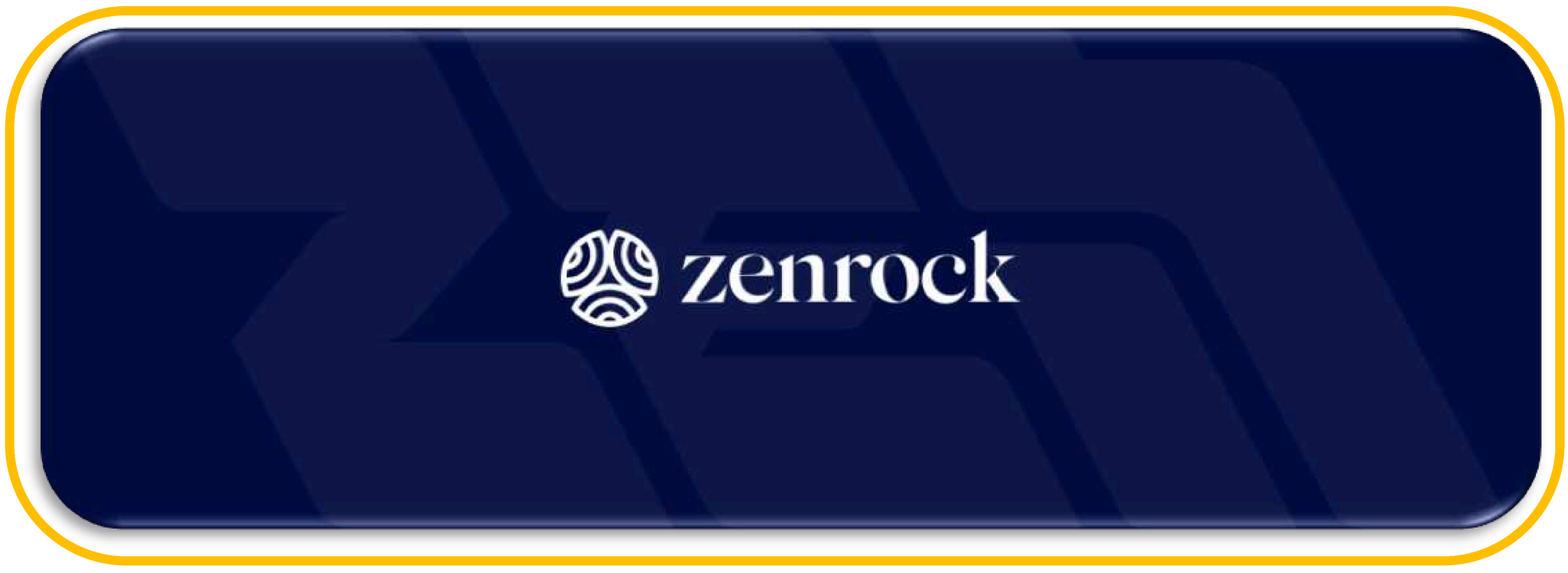
Because DCTs separate custody from execution, users never have to evaluate whether the underlying asset is safe.

It's secured by the Zenrock dMPC network and inherits all of the associated trust. By design.

So, while a specific wrapper might carry product or market specific risk, the custody doesn't.

This lets users **evaluate the product based on the product** and developers focus on creating something users want rather than complex back-end security.

Create a DCT and Earn



Interested in creating a DCT? Email: vip@zenrocklabs.io

One of the core innovations of the DCT standard is that **anyone can become a TVL provider.**

Through a simple developer interface, third parties can mint their own DCTs backed by any asset their users deposit into Zenrock's custody system — for example xyzBTC backed by BTC. The resulting token is a fully wrapped implementation secured by dMPC on zrChain. **From there, developers are free to build any additional features on top.**

The economic model is equally straightforward.

Each DCT contributes to the TVL on zrChain. At regular intervals, the protocol distributes a fixed share of all custody-related fees **(from all DCTs)** to TVL providers — proportional to their share of TVL.

For example, if xyzBTC represents 10% of all TVL held in custody, the issuer of xyzBTC receives 10% of the total fees allocated to TVL providers for that period (more on fee breakdown below). What they do with those rewards is entirely up to them: pass it to xyzBTC holders as native yield, route it to their governance token holders, retain it entirely, or anything else.

Importantly, **these rewards are not dependent on activity within their specific DCT.** Even if no users minted or burned xyzBTC during that window, the issuer still earns based on their TVL share. **This creates strong alignment: TVL providers benefit from the success of the whole ecosystem — not just their own slice — and are incentivized to grow their share of total collateral rather than drive churn through mint/burn activity in their DCT.**

By making custody composable and profitable, Zenrock turns what was once backend technology into a programmable, revenue-generating infrastructure.

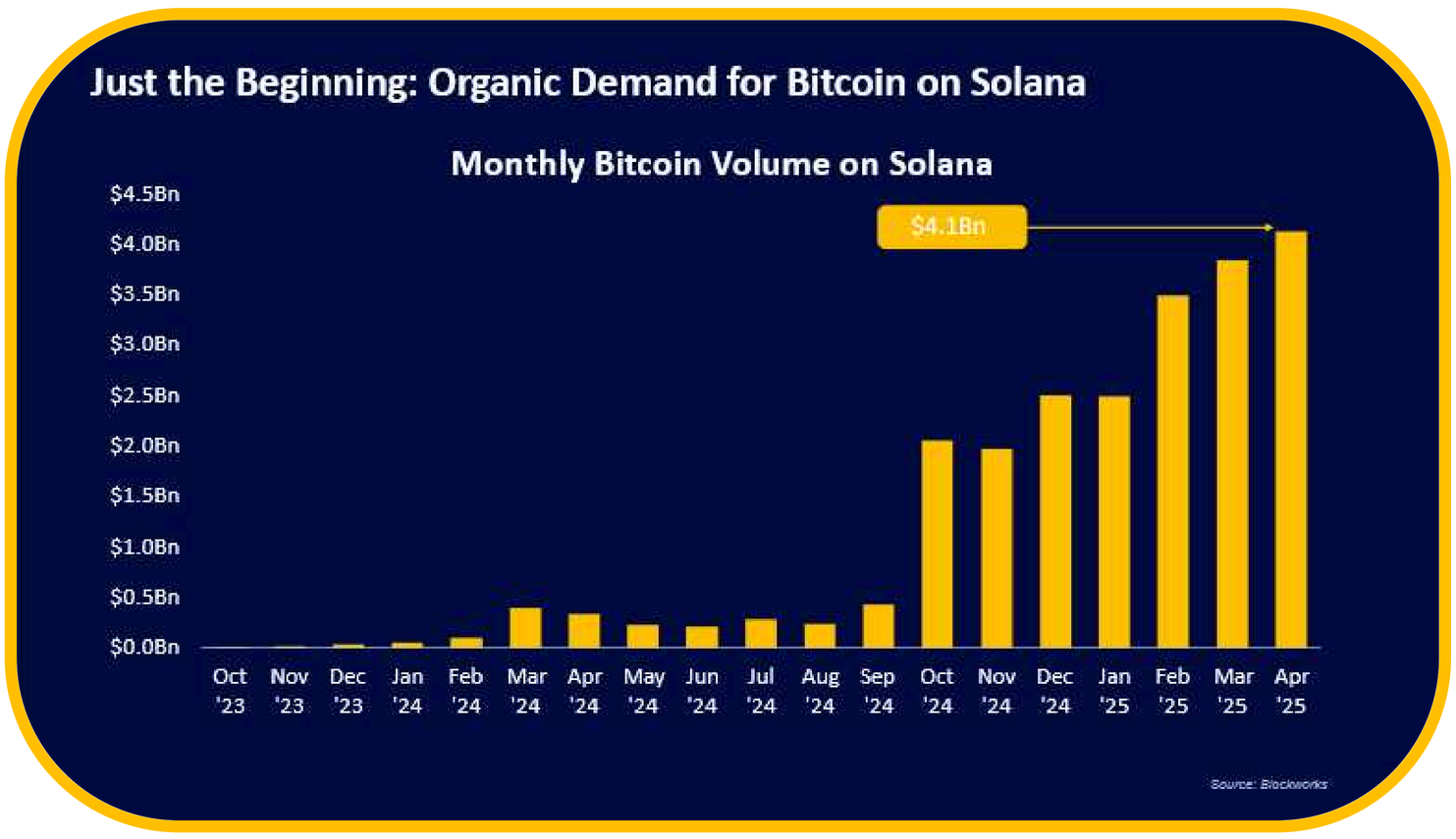
zenBTC: Decentralized, Secure Wrapped Bitcoin on Solana

Mint: https://zenbtc.app.zenrocklabs.io/

zenBTC CA: 9hX59xHHnaZXLU6quvm5uGY2iDiT3jczaReHy6A6TYKw

Bitcoin on Solana is absolutely exploding. **$4.1 billion in monthly volume in April 2025** alone is just the beginning. Bitcoin's $2.1 trillion market cap requires programmable access to DeFi.

Solana's speed and cost structure make it the perfect venue for leveraging Bitcoin's value onchain.

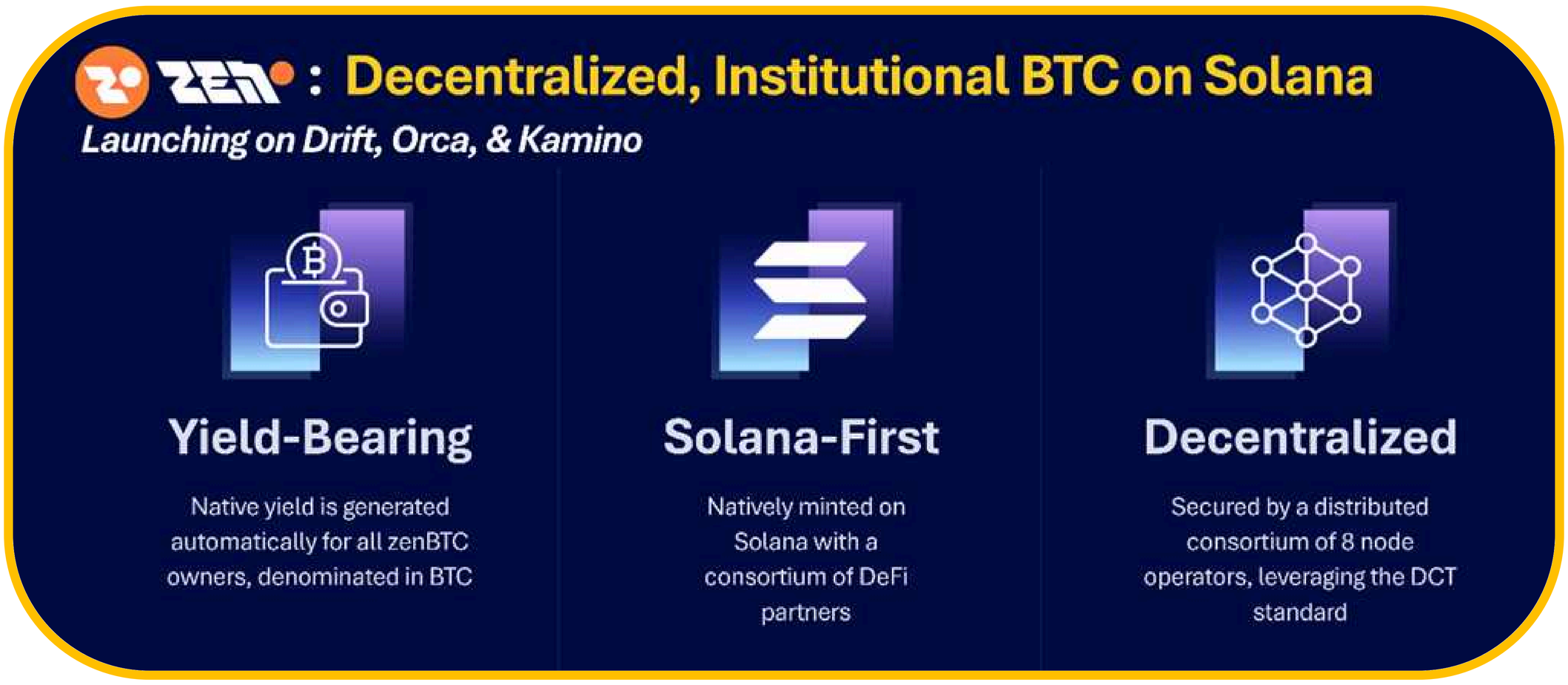


We expect that $4.1B volume to 10x within 8-12 months, given the adoption curves occurring across Solana DeFi.

The wrapped Bitcoin market on Solana will be measured in hundreds of billions within five years as Bitcoin is the primary asset viewed and used as collateral in DeFi.

The first asset built on the DCT standard is zenBTC — Zenrock's own wrapped Bitcoin product, purpose-built for **Solana**.

At its core, zenBTC is a DCT: a fully decentralized, MPC-secured representation of BTC. But zenBTC goes further.



zenBTC is designed to be the most secure, capital-efficient wrapped Bitcoin onchain.

Built for Solana, zenBTC leverages dMPC fees, restaking and other yield strategies to maximize utility.

All DCT fees earned by zenBTC on zrChain, are natively passed back to zenBTC holders as yield (more on this below).

zenBTC is poised to be the most powerful and composable BTC derivative possible — designed to take full advantage of Solana.

No lockups. No middlemen. Just Bitcoin that earns. Minted directly on Solana.

zrChain: A Purpose-Built Layer 1 Custody Network

zrChain is a Delegated Proof-of-Stake (DPoS) chain built on the Cosmos SDK standard that is the foundation of the Zenrock Protocol.

Backed by a globally distributed validator set with over **$100B in cumulative stake across 50+ chains, zrChain embodies the decentralization ethos.**

Zenrock launched with a genesis set of 8 dMPC operators (pictured above). Over time, the operator set will be expanded to 16 and then 32 operators — each time increasing the cryptographic threshold.

$ROCK: Fixed Supply, Deflationary by Design

Solana CA: 5VsPJ2EG7jjo3k2LPzQVriENKKQkNUTzujEzuaj4Aisf

zrChain CA: 0x83c82f0f959ad3eff528ee513b43808aa53f4b37

$ROCK, the native token of zrChain, serves both as the gas token and the governance token for the chain. **$ROCK exists both on Solana and Cosmos natively** (more on zenTP and $ROCK on Solana below). $ROCK has been implemented using Cosmos token standards, including the ICS-20 fungible token standard in the context of IBC.

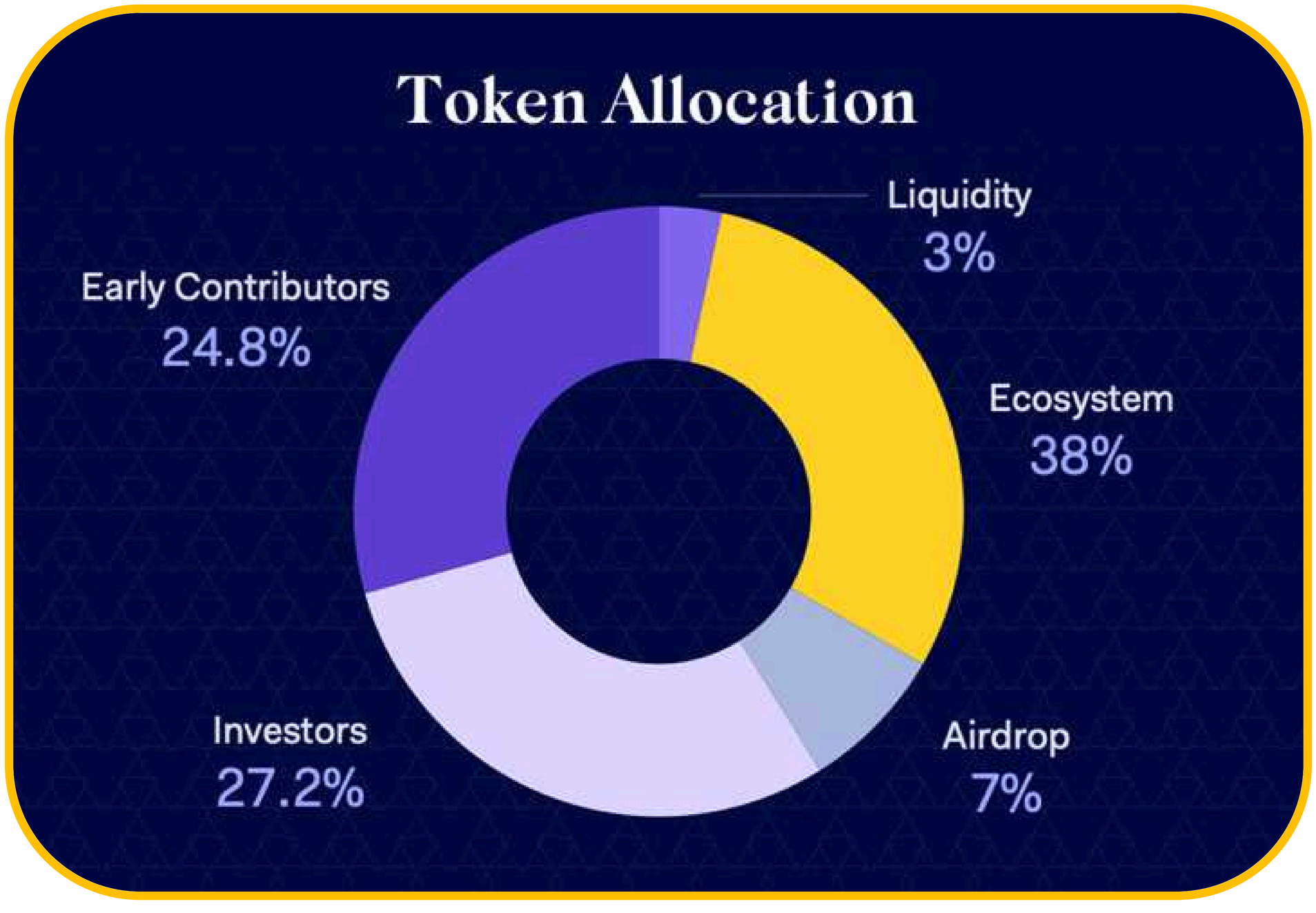
The **$ROCK** token has a **hard-capped supply of 1 billion tokens** — with no inflation, ever.

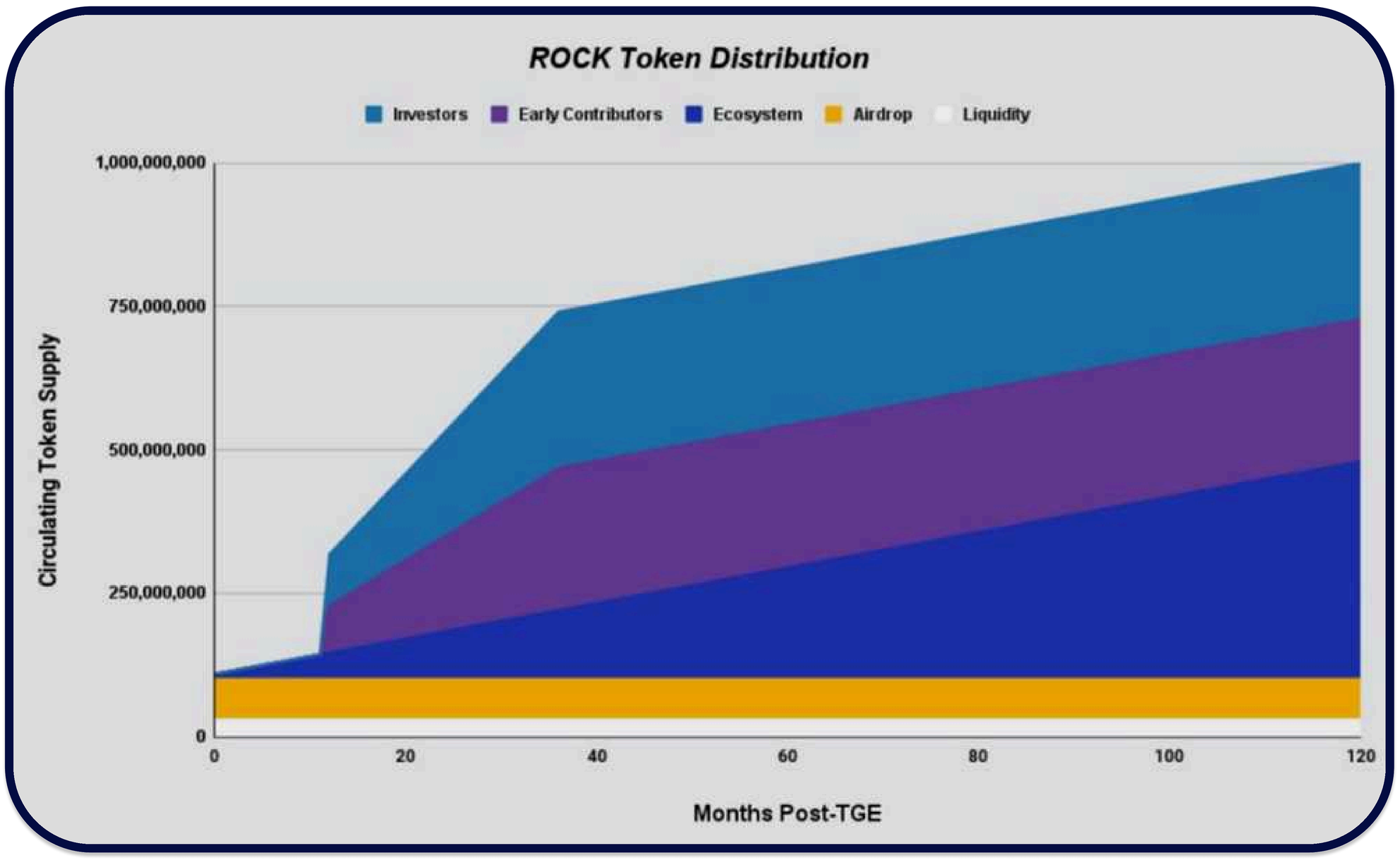
All rewards, incentives, and ecosystem grants are distributed from pre-allocated pools established at genesis. There is no mechanism to mint new tokens beyond this fixed supply.

$ROCK is designed to be **deflationary.** Every transaction on **zrChain** burns some $ROCK, reducing supply over time as network activity grows.

Despite having launched the first DCT, zenBTC, only a few weeks ago, zrChain has already burned over 5K tokens.

Below is a full breakdown of $ROCK token allocations at TGE, along with the vesting schedule for insiders and early contributors:


Token Allocation
Liquidity
3%
Early Contributors
24.8%
Ecosystem
38%
Investors
27.2%
Airdrop
7%


ROCK Token Distribution
Investors
Early Contributors
Ecosystem
Airdrop
Liquidity
1,000,000,000
750,000,000
500,000,000
250,000,000
0
Circulating Token Supply
0
20
40
60
80
100
120
Months Post-TGE

zenTP: The First Solana to Cosmos Bridge built on dMPC

Interested in using zenTP for your project? Email: vip@zenrocklabs.io

To make $ROCK accessible across chains, we built Zenrock Transfer Protocol, the first native bridge that connects Cosmos to Solana.

To seed initial liquidity, the Zenrock Foundation transferred **200 million $ROCK** to Solana. These are fully bridged, circulating tokens, represented as **$ROCK – an SPL token.**

As users move tokens back and forth between zrChain and Solana, the supply on each side will **fluctuate**, but the **total supply of $ROCK remains unchanged.**

Some Solana-based explorers or DEXs may incorrectly display the token's **fully diluted value (FDV)** by failing to account for the supply still on zrChain (likely the majority of tokens).

For an accurate picture, we recommend checking **CoinMarketCap** or **CoinGecko**, which reflect the full cross-chain supply.

zenTP ensures that $ROCK can move fluidly between ecosystems — without compromising security or supply integrity.

$ROCK Utility & Tokenomics

With the creation of zrChain we faced a second critical challenge: **how to design the economic system in a way that aligns every participant, rewards long-term contributors, and ensures the protocol can scale sustainably.**

The result is a tokenomic model centered around **$ROCK: a fixed-supply, deflationary asset that powers the chain, secures the network, and distributes value across the ecosystem.**

In the following sections, we'll walk through how zrChain tokenomics work under the hood, the role of $ROCK, and how rewards are shared between stakers, validators, infrastructure providers, and TVL providers.

This is the economic engine behind DCTs and why we believe it's built for the long run.

Unlike many other tokens in the web3 landscape, $ROCK had economic utility immediately upon TGE. This is due to Zenrock's node reward architecture and the fact that every dMPC key and signature request (actions that takes place when zenBTC or another DCT is minted, burned, or transferred cross-chain) produces fees into the node reward system.

When users pay fees in the form of $ROCK, those fees are stored in a reserve called the Node Reward Pool ("NRP"). The NRP is also the pool that distributes rewards to all stakers, validators, infrastructure providers, and TVL providers.

The Node Reward Pool: Core of the zrChain Economy

The NRP was **seeded at launch with 8% of total supply** (80 million $ROCK) by the Zenrock Foundation, giving the system multiple years of runway — even in the event that revenue is minimal. In addition, the Zenrock Foundation has allocated **10% more** of supply as reserves, if needed, to extend that runway further.

Of course, the long-term model is **fee-driven**, and we don't anticipate needing that additional 10%. But the design ensures resiliency: the protocol can operate, grow, and reward participants even before fees fully cover emissions, **and achieve this without inflation.**

Staking and the Surplus Model

All $ROCK staked on **zrChain** earns a **baseline 7% APR**, designed to provide predictable, protocol-aligned rewards to long-term participants.

Given this fixed yield, and the fixed base cost charged by MPC providers, we can calculate a **precise breakeven point** at any given block: the amount of revenue required to fully cover the network's reward obligations.

When revenue **falls short** this breakeven point, the protocol is in **deficit** — the NRP will cover the shortfall.

When revenue **exceeds** this breakeven point, the protocol enters **surplus** —and that unlocks a powerful set of mechanics of variable rewards.

Variable reward uses:

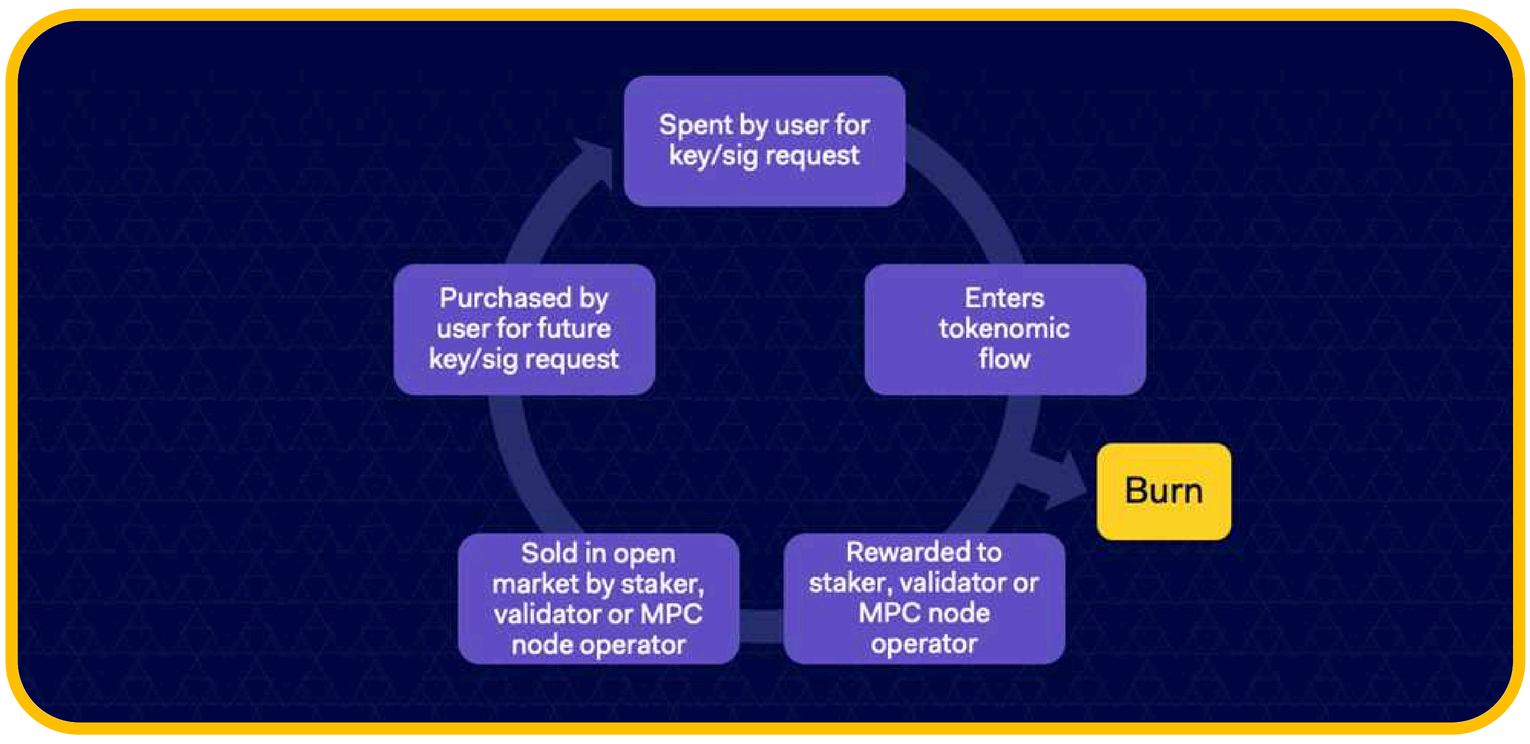
1. **Reserve Growth:** A portion of surplus $ROCK is retained in the **Node Reward Pool**, building long-term reserves for future volatility or slow periods.

2. **Token Burns:** Additional $ROCK is burned, increasing deflationary pressure and reducing total supply faster.

3. **Boosted Rewards:** Stakers, validators, infrastructure providers, and custody participants all receive **bonus rewards** above their base rates — amplifying incentives across the network.

In the event that the NRP grows substantially on the back of reserve growth through variable rewards, the Zenrock community has the option to burn or otherwise use the surplus tokens in the NRP at the direction of onchain governance.

The result is a system that's predictable in early stages, self-sustaining at maturity, and **accretive to $ROCK holders at scale. When zrChain is in surplus, everyone wins.**



Custody That Pays: How Fees Flow

One of the key features of the DCT standard is that **any third party can become a TVL provider** by minting their own DCT using Zenrock's custody infrastructure.

These TVL providers aren't just participants — **they're entitled to a share of the system's fee revenue.**

Here's how the fee flow works for zenBTC and other DCTs:

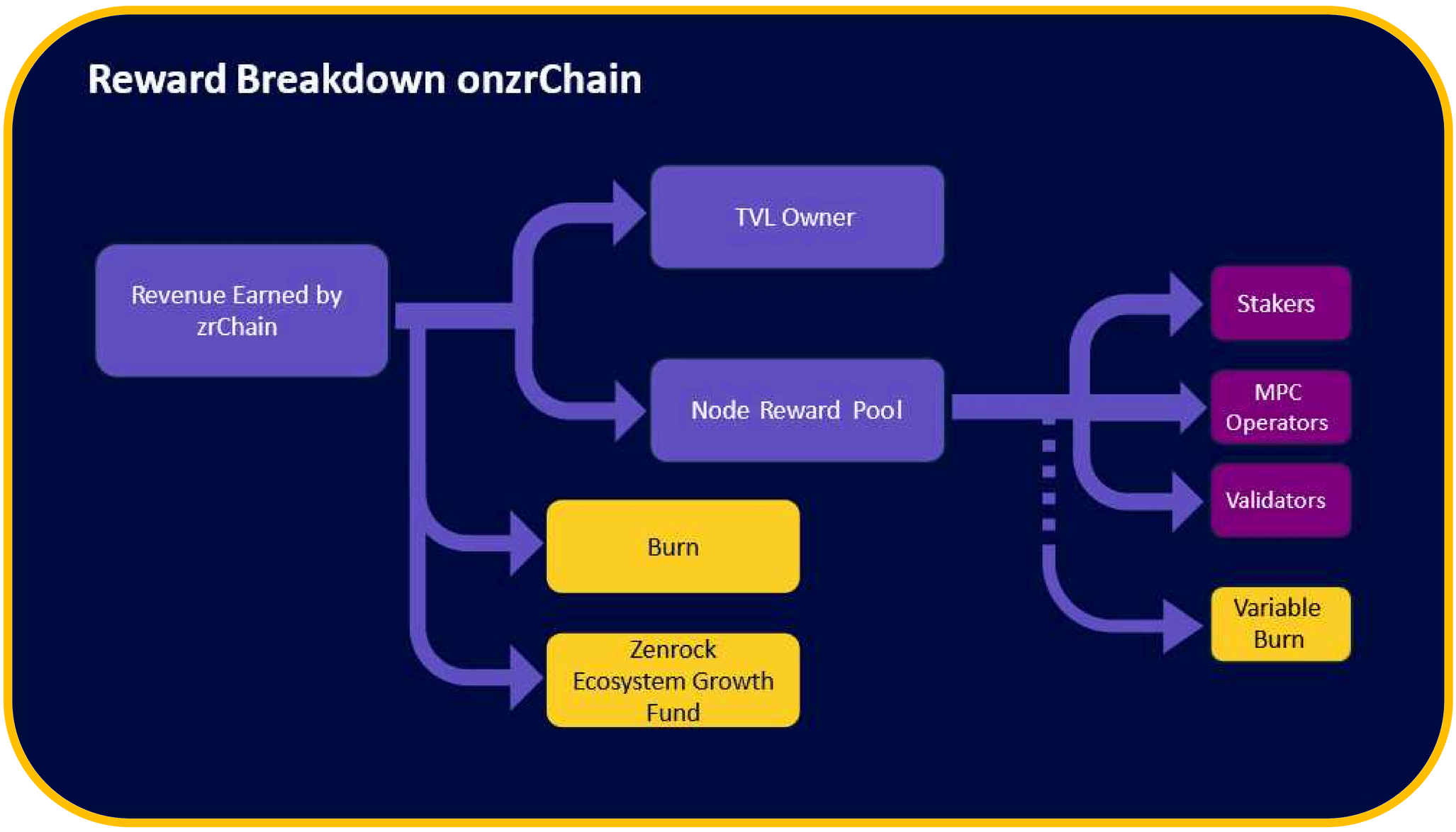
1. **10% of every fee is burned**, permanently reducing $ROCK supply.

2. **30% flows to the Zenrock Foundation Growth Fund**, used for future incentives and ecosystem development.

3. **30% flows to the TVL provider**—the party that supplied the BTC collateral. (In the case of zenBTC we pass that 30% back to users as yield)

4. **30% flows into the Node Reward Pool**, which pays rewards to stakers, validators, and MPC operators according to the system outlined above.

This architecture rewards everyone involved:



The Path Forward

Zenrock isn't just refining custody, we're revolutionizing it.

As more assets move across more chains, custody can no longer be a patchwork of ad hoc solutions. It needs to be standardized — robust, neutral, and trustless by design.

Build with us. Get started here: https://www.zenrocklabs.io/