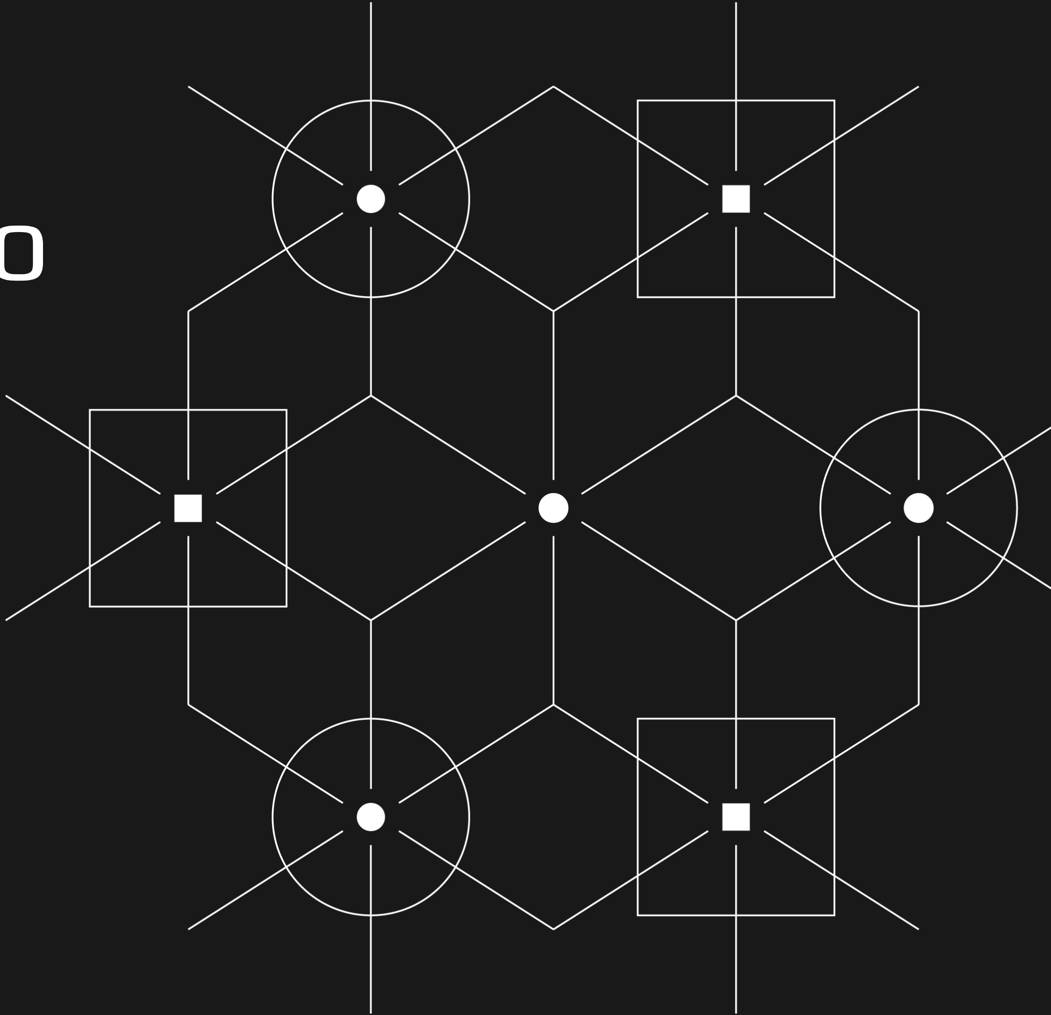
galaxy

What’s Going Into the Pectra Upgrade?



Christine Kim - Galaxy Research

www.galaxy.com/research

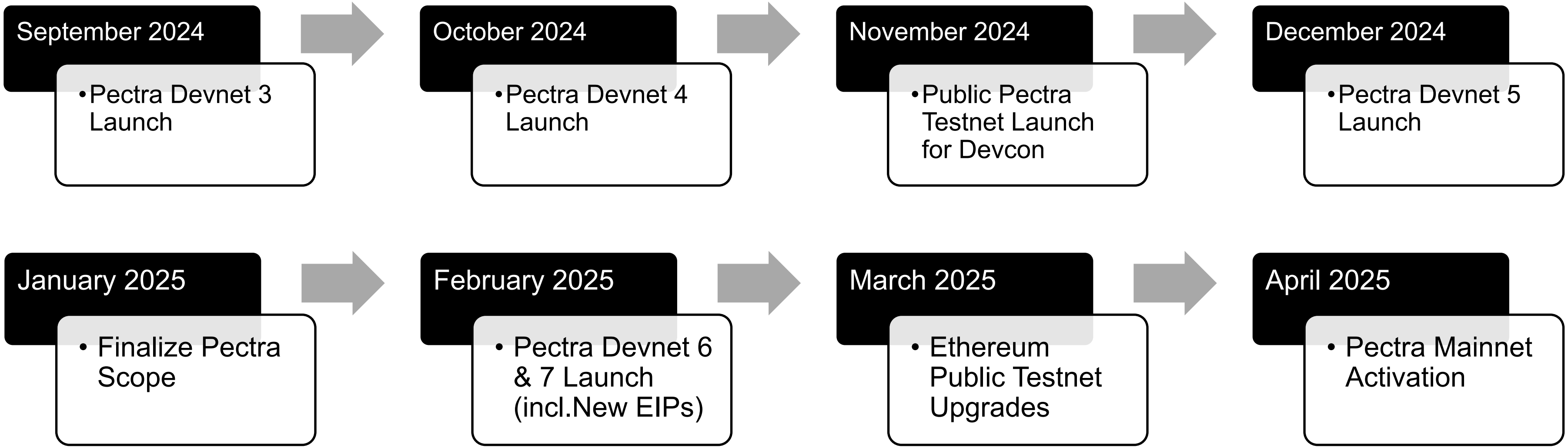
November 12, 2024

Disclaimer

This presentation, and the information contained herein, has been provided to you by Galaxy Digital Holdings LP and its affiliates ("Galaxy Digital") solely for informational purposes. This presentation may not be reproduced or redistributed in whole or in part, in any format, without the express written approval of Galaxy Digital. Neither the information, nor any opinion contained in this presentation, constitutes an offer to buy or sell, or a solicitation of an offer to buy or sell, any advisory services, securities, futures, options or other financial instruments or to participate in any advisory services or trading strategy. Nothing contained in this presentation constitutes investment, legal or tax advice. You should make your own investigations and evaluations of the information herein. Any decisions based on information contained in this presentation are the sole responsibility of the reader. Certain statements in this presentation reflect Galaxy Digital's views, estimates, opinions or predictions (which may be based on proprietary models and assumptions, including, in particular, Galaxy Digital's views on the current and future market for certain digital assets), and there is no guarantee that these views, estimates, opinions or predictions are currently accurate or that they will be ultimately realized. To the extent these assumptions or models are not correct or circumstances change, the actual performance may vary substantially from, and be less than, the estimates included herein. None of Galaxy Digital nor any of its affiliates, shareholders, partners, members, directors, officers, management, employees or representatives makes any representation or warranty, express or implied, as to the accuracy or completeness of any of the information or any other information (whether communicated in written or oral form) transmitted or made available to you. Each of the aforementioned parties expressly disclaims any and all liability relating to or resulting from the use of this information. Certain information contained herein (including financial information) has been obtained from published and non-published sources. Such information has not been independently verified by Galaxy Digital and, Galaxy Digital, does not assume responsibility for the accuracy of such information. Affiliates of Galaxy Digital own investments in some of the digital assets and protocols discussed in this webinar. Except where otherwise indicated, the information in this presentation is based on matters as they exist as of the date of preparation and not as of any future date, and will not be updated or otherwise revised to reflect information that subsequently becomes available, or circumstances existing or changes occurring after the date hereof. The foregoing does not constitute a "research report" as defined by FINRA Rule 2241 or a "debt research report" as defined by FINRA Rule 2242 and was not prepared by Galaxy Digital Partners LLC.

Tentative Pectra Timeline Analysis

Source: Galaxy Research



September 2024

- Pectra Devnet 3 Launch

October 2024

- Pectra Devnet 4 Launch

November 2024

- Public Pectra Testnet Launch for Devcon

December 2024

- Pectra Devnet 5 Launch

January 2025

- Finalize Pectra Scope

February 2025

- Pectra Devnet 6 & 7 Launch (incl.New EIPs)

March 2025

- Ethereum Public Testnet Upgrades

April 2025

- Pectra Mainnet Activation

Pectra EL EIPs

EIP #	EIP Authors	EIP Created	EL or CL-focused?	Title	Expected Impact
2537	Alex Vlasov, Kelly Olson, Alex Stokes, Antonio Sanso	2020-02-21	EL	Precompile for BLS12-381 curve operations	Adds new functions to efficiently perform operations over the BLS12-381 curve, which is an algebraic structure widely used for zero-knowledge cryptography. Zero-knowledge cryptography can offer several benefits for blockchain-based applications, including stronger privacy guarantees, security, and scalability.
2935	Vitalik Buterin, Tomasz Stanczak, Guillaume Ballet, Gajinder Singh, et al.	2020-09-03	EL	Serve historical block hashes from state	This code change introduces a change to the EL such that proofs of historical blocks can be generated from the state. (State refers to the current balances of all Ethereum accounts, the contract code that controls them, and storage data.) It is required for the Verkle transition and stateless clients. It also offers some benefits for light client syncing and enables smart contracts to utilize information about state from historical blocks via the EVM.
7685	Lightclient	2024-04-14	EL	General purpose execution layer requests	More efficient way to code, test, and implement execution triggered requests like EIP 6110 and EIP 7002.
7702	Vitalik Buterin, Sam Wilson, Ansgar Dietrichs, Matt Garnett	2024-05-07	EL	Set EOA account code	Introduces more flexibility to user-controlled accounts, EOAs, by enabling account features like transaction batching, sponsored transactions, conditional transactions, and delegated security.

Pectra CL EIPs

EIP #	EIP Authors	EIP Created	EL or CL-focused?	Title	Expected Impact
7742	Alex Stokes	2024-07-12	CL/EL	Uncouple blob count between CL and EL	Introduces a mechanism to dynamically set blob gas targets and max limits through the CL.
6110	Mikhail Kalinin, Danny Ryan, Peter Davies	2022-12-09	CL	Supply validator deposits on chain	Removes the need for deposit voting from the Consensus Layer and thereby reduces complexity of client software design. It also improves validator UX by decreasing delay between submitting a deposit tx on EL and seeing it processed on CL.
7002	Danny Ryan, Mikhail Kalinin, Ansgar Dietrichs, Hsiao-Wei Wang, et al.	2023-05-09	CL	Execution layer triggerable withdrawals	Allows validators to trigger exits and partial withdrawals via their execution layer (0x01) withdrawal credentials. This enables more trustless staking pool designs on Ethereum.
7251	Mike Neuder, Francesco, dapplion, Mikhail Kalinin, et al.	2023-06-28	CL	Increase the MAX_EFFECTIVE_BALANCE	Allow validators to have larger effective balances, while maintaining the 32 ETH lower bound. This reduces the growth of the validator set size and thereby improves the security and health of the network.
7549	dapplion	2023-11-01	CL	Move committee index outside Attestation	Makes the aggregation of validator votes (i.e., attestations) in blocks more efficient, this in turn reduces networking load and saves node bandwidth.
TBD	TBD	TBD	CL	Increase blob target and max limit	Increases data availability capacity such that costs to post data to Ethereum by Layer-2 rollups becomes cheaper.

Pectra Outlook

In aggregate, Pectra contains a mixed bag of updates to Ethereum that are expected to achieve three outcomes:

1. Fix critical shortcomings of the protocol as a proof-of-stake blockchain
2. Improve the user experience (UX) of interacting with smart contract applications on Ethereum
3. Increase Ethereum’s data availability capacity

EIPs Removed from Pectra

EIP #	Title	Description
7549	Introducing simple DAS utilizing gossip distribution and peer requests	Improve Ethereum's capacity to scale through Layer-2 rollups. It implements a new networking protocol to increase blob capacity while keeping the computational load on nodes unchanged.
663	SWAPN, DUPN and EXCHANGE instructions	All EVM operations are executed from a data area known as "the stack". It has a maximum capacity of 1024 elements. instructions to access and perform operations on these stack elements are limited to a stack depth of 16. The creation of SWAPN, DUPN, and EXCHANGE instructions enable smart contract developers to access deep stack items with a single instruction, thereby reducing the complexity and cost of smart contract code.
3540	EVM Object Format v1	Creates a structure for the EVM to analyze smart contract code. It adds a version field, which developers can use to introduce new features to the EVM and deprecate old ones in a backwards-compatible way. It also creates a field for smart contract code and a field for smart contract data. The differentiation between code and data is useful for testing and formal verification of smart contracts.
3670	Code validation	Introduces basic code validation at contract creation time.
4200	Static relative jumps	Creates three new EVM jump instructions for altering the sequence of smart contract code execution more accurately and efficiently. Deprecates the older method for altering the path of code execution known as "dynamic jumps".
4750	Functions	Creates additional structure for the EVM to support subroutines.
5450	Stack validation	Introduces extended validation of code sections to guarantee that neither stack underflow nor overflow can happen during execution of validated contracts.
6206	JUMPF and non-returning functions	Creates instructions that allow altering the sequence of code execution without needing to update or add a new return stack frame.
7069	Revamped CALL instructions	Creates three new call instructions, EXTCALL, EXTDELEGATECALL and EXTSTATICCALL, with simplified semantics for loading return data into the stack. Deprecates the older method for loading return data through CALL operations and the GAS opcode.
7480	Data section access instructions	Creates instructions for smart contract developers to read and access information in the data field of an EOF container efficiently in lieu of deprecated opcodes in EIP 3540.
7620	EOF contract creation	Deprecates CREATE and CREATE2 instructions for creating new smart contracts and replaces these instructions with new ones that utilize the structure of EOF containers.
7698	Creation transaction	A mechanism for deploying EOF smart contracts.

Potential Fusaka EIPs

Title	EIP #	Description	Expected Impact
“EOF”	Various	A bundle of 11 EIPs changing how EVM bytecode is processed and executed on Ethereum	Improvement to the dapp developer experience that will make EVM smart contract code execution more efficient, predictable, logically sound, and upgradeable.
PeerDAS	7549	Introducing simple DAS utilizing gossip distribution and peer requests	Improve Ethereum’s capacity to scale through Layer-2 rollups. It implements a new networking protocol to increase blob capacity while keeping the computational load on nodes unchanged.
Verkle Transition	TBD	Update Ethereum’s data structure for state to Verkle	This will allow for smaller proof sizes which are necessary for supporting stateless clients. Reduced state size from Verkle will also mean lower hardware requirements to run a node, which improves decentralization.
Full SSZ Transition	6404, 6493	Migration of RLP transactions to SSZ Signature scheme for native SSZ transactions.	RLP, the data serialization method used for transactions on the EL, has several shortcomings and it is not the same method used for transactions on the CL. To normalize transaction representation across both the CL and EL and improve serialization methods on the EL, these EIPs will convert all RLP transactions to SSZ.
Inclusion Lists	7547	Add an inclusion list mechanism to allow forced transaction inclusion.	Censorship resistance is a core value proposition of blockchains. Inclusion lists aim to provide a mechanism to improve the censorship resistance of Ethereum by allowing proposers to specify a set of transactions that must be promptly included for subsequent blocks to be considered valid.
Stake Ratio Targeting	TBD	An adjustment to the issuance policy.	Mitigates the negative externalities associated with a high staking ratio like inducing more demand for liquid staking tokens.
History Expiry	7639	Block history takes up a lot of space on nodes and once a block has been finalized, it is only needed for limited use cases that are not critical to network consensus.	Block history will no longer be stored permanently by full nodes. After some period, it will be removed from nodes, and entities that need it, can query for it from another source such as the Portal Network.
Enshrined Proposer Builder Separation (ePBS)	7732	Separates the Ethereum block in consensus and execution parts, adds a mechanism for the consensus proposer to choose the execution proposer.	It removes the need to use trusted middleware to delegate block construction to a builder and thereby improves the decentralization and censorship resistance of Ethereum.
Account Abstraction	TBD	Migrate user-controlled accounts, also called externally owned accounts (EOAs) to smart contract accounts.	Increases the flexibility of asset management and custody when user assets are stored in smart contracts, instead of EOAs. Transaction authorizations are not limited to a private key signature. These authorizations can be programmable to make for a safer and more user-friendly Web3 experience.

Thank you for listening!

Christine Kim - Galaxy Research

www.galaxy.com/research

X: @christine_dkim