Shangai Fork:
O próximo passo da Ethereum

MB Research

Introdução

Desde seu lançamento em julho de 2015, era evidente que a Ethereum precisaria de várias atualizações ao longo dos anos. Além disso, com o passar do tempo, a evolução de diversas tecnologias, novas demandas, problemas e soluções foram surgindo, forçando os desenvolvedores e membros da comunidade a adaptar o blockchain para os mais diversos desafios do mundo real.

Os desafios de criar um blockchain *general purpose* utilizado por centenas de milhões de pessoas e ao mesmo tempo seguro e moderno é imenso. Centenas e agora milhares de desenvolvedores precisam coordenar seus trabalhos, estipular prazos realistas (algo que já é complexo para pequenos projetos de *software*, imagina para um desta magnitude) e ainda assegurar que nada de errado ocorrerá com os bilhões de dólares travados na rede.

Todo esse esforço demandou um processo de maturação dos times de aplicações e da própria Ethereum Foundation, que guia o desenvolvimento, apesar de não possuírem em nenhuma instância a posse do protocolo.

Como tradição na rede, temos um nome que representa as atualizações na camada de execução e um para a camada de consenso. Para as camadas de execução, são dados os nomes das cidades, para a camada de consenso, são utilizados nomes de estrelas.

Shanghai Fork: atualizações na camada de Execução da Ethereum
Capella Fork: atualizações na camada de Consenso da Ethereum

Muitas vezes os desenvolvedores, para simplificar, se referem aos *forks* por uma aglomeração de seus nomes, nesse caso: **Shapella**.

Entendendo o *fork*

Para entendermos o Shapella Fork, precisamos primeiro dar um passo atrás e entender melhor a última atualização da Ethereum, o The Merge, que ocorreu no dia 15 de setembro de 2022.

Com a ideia da migração do *Proof-of-Work* para o *Proof-of-Stake*, os desenvolvedores do protocolo base da Ethereum decidiram que a responsabilidade de consenso entre os nós e a execução das transações e contratos inteligentes seria separada.

Para tal, criaram, em dezembro de 2020, a Beacon Chain, atual camada de consenso da rede da Ethereum. Essa camada ficaria inoperante até o momento do Merge, mas já aceitaria depósitos de etheres pelos futuros validadores, justamente para que a transição pudesse ser feita posteriormente.
A camada, porém, não permitia o **saque** desses etheres, e esse é o grande ponto em que entra o Shapella Fork.

Os validadores também começaram a ser recompensados com etheres, mesmo que ainda não estivessem envolvidos diretamente com a validação, e isso foi feito para atrair depósitos de ether para o contrato da Beacon Chain. Abordaremos mais sobre isso na seção correspondente.

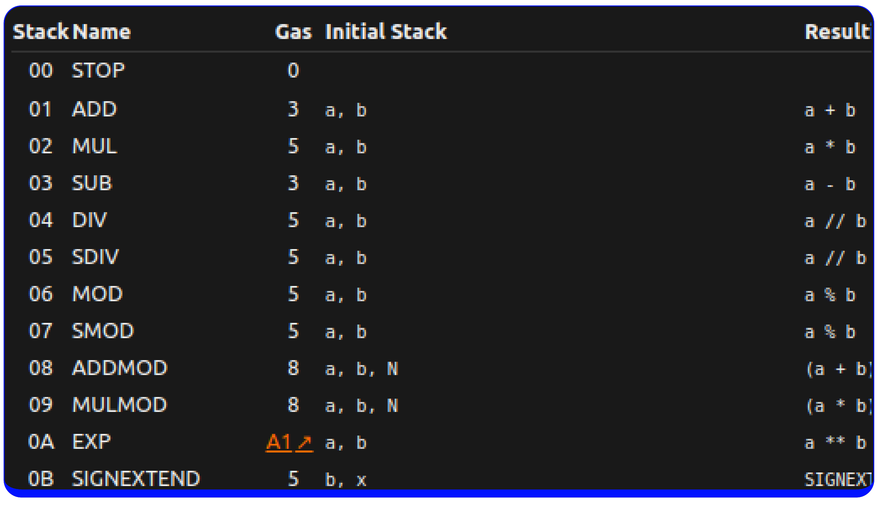
Além deste ponto, para entendermos as outras EIPs envolvidas, é necessário o entendimento do conceito de OPCODES.

Os **OPCODES** são como são conhecidos os códigos das operações-base que a EVM *(Ethereum Virtual Machine)* executa. Todo e qualquer contrato inteligente - independentemente de sua complexidade - pode ser quebrado em pequenas operações básicas, que são interpretadas pela EVM.

Essas operações são utilizadas como base para o cálculo de *gas* (medida de custo computacional necessário para se realizar as operações desejadas) a ser utilizado para a execução do contrato.

Uma operação de adição entre dois inteiros, por exemplo, custa 3 unidades de *gas*. Uma operação lógica OU, custa também 3 unidades de *gas* para ser executada, e assim por diante.

O leitor pode encontrar a lista completa de OPCODES e seus custos, bem como *inputs*, *outputs* e operações aqui.



Stack	Name	Gas	Initial Stack	Result
00	STOP	0		
01	ADD	3	a, b	a + b
02	MUL	5	a, b	a * b
03	SUB	3	a, b	a - b
04	DIV	5	a, b	a // b
05	SDIV	5	a, b	a // b
06	MOD	5	a, b	a % b
07	SMOD	5	a, b	a % b
08	ADDMOD	8	a, b, N	(a + b)
09	MULMOD	8	a, b, N	(a * b)
0A	EXP	A1↗	a, b	a ** b
0B	SIGNEXTEND	5	b, x	SIGNEXT

Exemplos de alguns OPCODES da EVM, com seus custos de gas e operações executadas.
Fonte: https://ethereum.org/en/developers/docs/evm/opcodes/

Shapella Fork

Chegamos finalmente ao ponto de interesse: a próxima atualização da Ethereum.

A principal motivação para o fork é permitir a liberação de saques de etheres travados para validação na Beacon Chain, porém, outras EIPs menores também serão incluídas nesse pacote.
Nesta seção, vamos abordar uma-a-uma as EIPs que serão incluídas nesse fork, bem como suas aplicações e explicações:

EIP-3651: Warm COINBASE

Para realmente entender essa EIP, precisamos entender outra anterior, a EIP-2929. Esta EIP, proposta pelo próprio Vitalik, foi uma solução rápida para um problema observado na rede.

Estavam ocorrendo ataques de DoS *(Denial of Service)* na qual o atacante busca sobrecarregar um servidor ou uma rede por meio de uma enxurrada de requisições e/ou transações. Nos ataques de 2016, um atacante conseguiu fazer isso a um custo relativamente baixo, enviando diversos endereços para serem inicializados nas transações.

Para driblar essa estratégia, a EIP-2929 determinou que apenas os endereços *ORIGIN* (originador da transação) e tx.to (receptor da transação) fossem carregados inicialmente, sendo mais baratos por isso, e que quaisquer outros endereços tivessem um custo adicional de *gas* para serem carregados. Em termos financeiros, isso limitaria a quantidade de endereços que poderiam ser enviados nas transações, resolvendo o problema em questão.

Acontece que existe outro endereço que é importante de ser inicializado, o que é responsável pela recompensa do bloco e das taxas de transação, chamado de *COINBASE*.

Essa proposta, então, se resume a incluir esse endereço na lista dos endereços inicializados assim que a transação começa, reduzindo seu custo, mas ainda mantendo a segurança contra os ataques de DoS.

EIP-3855: PUSH0 instruction

Essa EIP é bem simples, sua proposta é de incluir uma nova instrução *(PUSH0*) que insere o valor constante zero na stack. Existem diversos motivos para se querer disponibilizar essa constante, mas principalmente para operações com instruções do tipo *CALL* (ex. *CALLDATA*).

Hoje em dia, desenvolvedores utilizam soluções alternativas para obter esse resultado, como executar a instrução *PUSH1 0*, que obtém o resultado desejado, mas sua execução é mais cara. Estudos na própria blockchain (ver link da EIP) estimam que cerca de 11,5% dos casos das instruções PUSH tem como objetivo final inserir um zero na stack.

Com o *PUSH0*, pretende-se resolver esse problema e tornar os códigos mais baratos e mais seguros, pois há menos chances de efeitos colaterais que podem ocorrer quando se usa uma solução alternativa.

EIP-3860: Limit and meter initcode

Essa EIP tem como objetivo medir e limitar o tamanho máximo do *INITCODE*.
O *INITCODE* é o bytecode de criação (código de máquina) gerado pelo *client* ao começar a criar um contrato em blockchain. Hoje em dia não há limite de tamanho máximo para o INITCODE e, na verdade, seu tamanho nem é mesmo medido.

Essa atualização busca resolver justamente esses dois pontos: implementar um sistema de medição do INITCODE e limitar seu valor máximo.

O novo máximo será de 49152 bytes,definido como o dobro do MAX_CODE_SIZE, e será aplicado custo extra de 2 gas para cada 32 bytes utilizados.

EIP-6049: Deprecate SELFDESTRUCT

Um dos OPCODES existentes é o **SELFDESTRUCT**, responsável por tornar inutilizável um contrato *deployado* em blockchain. Essa EIP insere apenas uma **advertência** ao uso do *opcode,* já que o comportamento do mesmo não será alterado nesse *fork*, mas é esperado que seja
alterado futuramente.

EIP-4895: Beacon Chain push withdrawals as operations

Finalmente, por último e mais importante, temos a EIP-4895, que implementará a já citada possibilidade de se realizar saques na Beacon Chain.

Apesar da funcionalidade ser simples, suas consequências podem ser grandes para a rede. Atualmente, existem cerca de 16.900.000 etheres travados em *stake* no contrato da Beacon Chain, como vemos abaixo:

Evolução da quantidade de etheres em stake na Beacon Chain desde seu surgimento.
Fonte: Glassnode

Essa quantidade equivale a cerca de 14% do *supply* total de etheres, um valor relativamente baixo quando comparado a outros blockchains. Uma análise interessante é quanto que os destravamentos destes etheres afetarão o preço do ativo. Elencamos argumentos que defendem a queda no preço e outros que argumentam que ele se manterá normal. Vamos analisá-los a seguir.

Argumentos pró-queda

O principal argumento dessa categoria é simples de entender. Com a possibilidade de sacar os etheres (liquidez), muitos dos *holders* tenderão a se desfazer pelo menos de parte de suas posições pois estão acumulando pagamentos desde o final de 2020.
Isso a princípio geraria uma pressão de venda que derrubaria o preço.

Podemos avaliar esse ponto por meio dos dois movimentos possíveis por parte dos validadores:

- Validadores que farão retiradas parciais (**Partial Withdrawals/PW**) - estes retirarão apenas as recompensas obtidas ao longo desse período, mantendo a quantidade mínima para ser um validador ainda travada (32 etheres x número de validadores).

- Validadores que farão retiradas totais (**Full Withdrawals/FW**) - estes retirarão a totalidade dos fundos, não só as recompensas obtidas, mas também os etheres travados para poderem se tornar um validador.

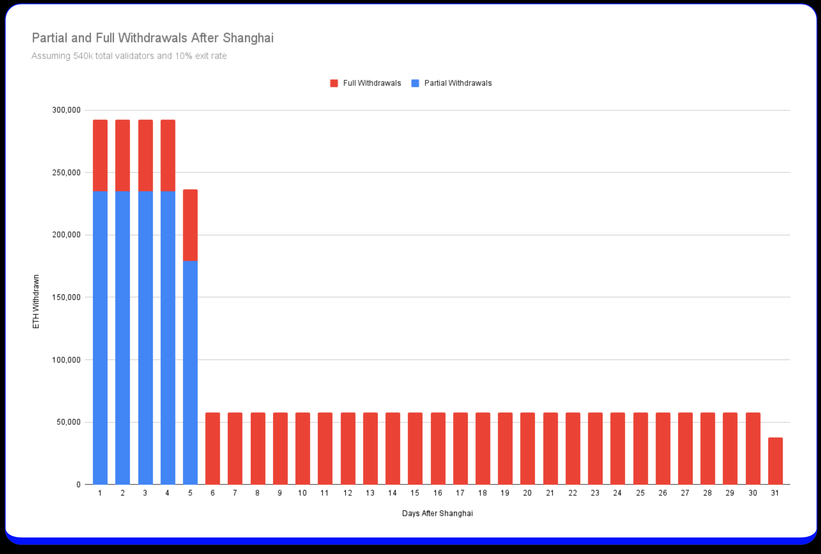
Observe que teremos *holders* que podem sacar seus etheres, mas não os venderão a mercado, utilizando-os para outras aplicações ou até mesmo para *hold* puro.

Outro ponto importante é devido a segurança da rede, já que não será permitido automaticamente que todos os validadores desmontem suas posições totais (FW), apenas cerca de um validador por minuto poderá abandonar a rede por vez, o que totalizará cerca de 1.500 validadores por dia (ou cerca de 50.000 etheres/dia).

É provável que no início tenhamos uma quantidade considerável de validadores buscando liquidez, até mesmo porque alguns já desmontaram seus nós e estão na fila para poder sacá-los.

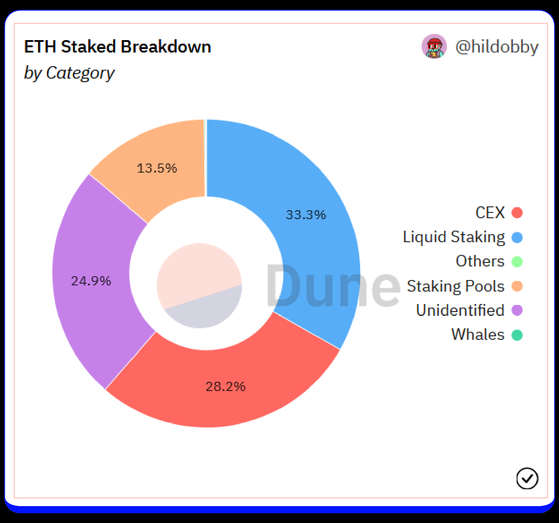
Estudos demonstram que, ao final de março (quando ocorrerá a atualização) considerando a retirada de todos os etheres em PW, teríamos um saldo de cerca de 1.119.000 etheres sendo retirados e considerando 10% do FW sendo processados, mais 1.728.000 etheres saindo da Beacon Chain. Somando todos esses números, e incluindo os validadores que já desativaram seus nós, resultam em mais 38.000 etheres que serão retirados.

Finalmente, a retirada estimada será de 2.885.000 etheres, um valor que corresponde a 2,4% do *supply* total, divididos a cada dia e também respeitando o limite máximo de retiradas por dia.



Simulação de saques na Beacon Chain dia-a-dia até um mês pós-Shanghai Fork.
Fonte: Twitter

As retiradas não necessariamente significam a venda do ativo,que é o fator que influencia no preço). Para entender quanto provavelmente será vendido, precisamos avaliar o perfil dos holders em questão:



Perfil dos holders de etheres em stake.
Fonte: Dune Analytics

Percebemos quatro grandes perfis de *holders* com quantidades referentes a cada perfil listadas abaixo:

- 33.3% Staking Líquido (Lido,Rocketpool, etc)
- 28.2% Exchanges Centralizadas (Coinbase, Binance, etc)
- 25.0% Outros (Não-identificados, baleias, outros)
- 13.5% Pools de Staking

Para os *holders* que se encaixam na categoria de Staking Líquido, não é esperada venda em quantidades consideráveis, pois esses *holders* já têm acesso a liquidez devido aos recibos recebidos ao terem realizado o depósito inicialmente.

Para os participantes das *Pools de Staking*, é esperado movimento de venda em pequenas quantidades, pois de modo geral esses holders estão alinhados à atividade de validação e acreditam no futuro da rede.

Para os *holders* em Exchanges Centralizadas, o cenário é similar ao descrito para os *Pools de Staking, pressão de venda razoável, mas não muito grande.*

E, finalmente, o grupo dos 'outros' que são em sua maioria validadores individuais, muito alinhados com a rede e que acredita-se que exista uma pressão de venda por realização de lucros, mas não em grande quantidade.

Considerando esses pontos, podemos traçar três cenários para as vendas dos PW:

Otimista: 8% => 92.000 ETH
Médio: 16% => 183.000 ETH
Agressivo 30% => 333.000 ETH

Já para os FW nessas categorias, nesses mesmos três cenários:

Otimista: 2% => 345.000 ETH
Médio: 7% => 1.206.000 ETH
Agressivo: 15% => 2.585.000 ETH

Totalizando, então, uma pressão de venda total de:

Otimista => 437.000 ETH
Médio => 1.389.000 ETH
Agressivo => 2.918.000 ETH

Que considerando a limitação de saques, representarão uma pressão de venda diária média de:

Otimista => 14.000 ETH por dia, por um mês
Médio => 23.000 ETH por dia, por dois meses
Agressivo => 32.000 ETH por dia, por três meses

O cenário otimista tem uma pressão de venda média diária muito similar ao que ocorria pré-Merge, quando os mineradores vendiam os etheres minerados, nada fora do comum.

Já os cenários médio e agressivo são consideravelmente maiores e mais duradouros, podendo levar a uma queda no preço do ativo caso não entrem novos validadores.

Argumentos contra a queda

Alguns dos principais argumentos contra a queda já foram elencados na seção anterior, nomeadamente:

Muitos dos *holders* estão para o longo prazo e são alinhados com o *ethos* da rede, não tendendo a se desfazer de suas posições e, possivelmente, até começando a rodar novos nós.

Muitos outros já têm acesso à liquidez, devido aos derivativos de Staking Líquido. *Traders* de curto e médio prazo provavelmente já fazem arbitragem e outras negociações em cima desses derivativos, não apresentando tanta tendência em vender seus ativos se não for por uma necessidade iminente de liquidez.

Além disso, grande parte dos etheres depositados foi feito quando o preço do ativo se encontrava em um patamar superior ao atual e acredita-se que esses *holders* terão menos tendência a vender o ativo pois estariam no prejuízo. Obviamente essa parcela varia muito dependendo de quanto tiver o preço do ether no pós-fork, mas extrapolando o crescimento atual, não é esperado que atinja grande quantidade percentual.

Shapella em *testnets* e *Shadow Forks*

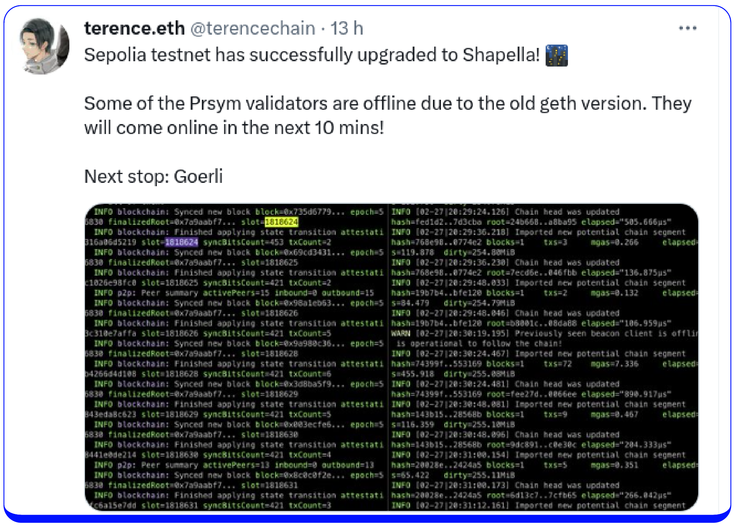
Assim como tivemos no The Merge, temos todo um roadmap de testes para a atualização que contará com *shadow forks* e atualizações em *testnets* antes da atualização final na *mainnet*.

Primeiramente, foram realizados *shadow forks* da mainnet. Essas redes são 'cópias' da rede principal que são separadas da *mainnet* e só permitem desenvolvedores como validadores. Nessas cópias, então, são realizadas as atualizações e os devs procuram *bugs* e outros problemas que podem ter ocorrido durante o processo. Mais outros *shadow forks* estão planejados até a execução da atualização na rede principal.

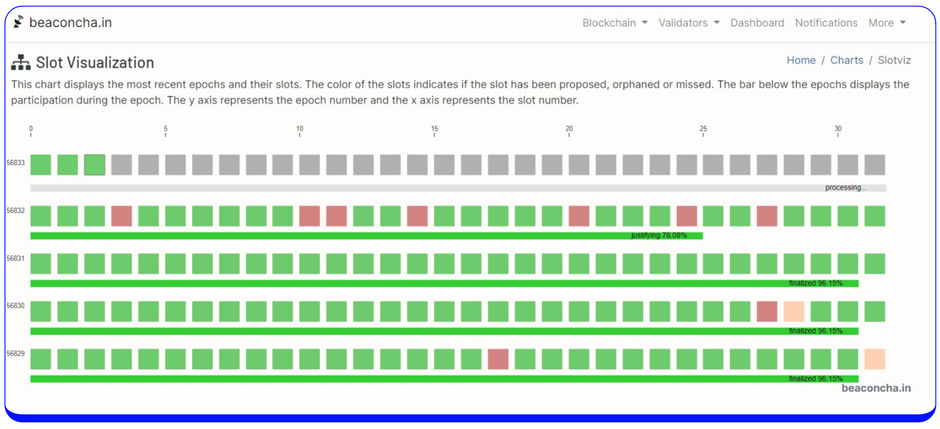
Em seguida, foi criada uma *testnet* (Zhejiang) para a realização da atualização e houveram alguns problemas de configurações em *clients* que foram rapidamente resolvidos. A *testnet* está funcional e os saques já podem ser testados por lá.

O passo seguinte foi a realização da atualização na *testnet* da Sepolia, que foi realizada com sucesso na madrugada do dia 28/02 (cerca de 4:04h UTC). Apesar da participação ter caído no momento do *fork* a cerca de 80%, esse valor ainda é considerado seguro, tendo como *threshold* mínimo o valor de 67%.

Tweets dos desenvolvedores afirmaram que a queda se deu principalmente devido a perda de sincronia de alguns nós que rodavam validadores da *Prysm*, que estavam com uma versão antiga do *client geth*, algo que foi rapidamente corrigido e, em pouco tempo, fez com que a participação subisse novamente para o patamar normal de 96%.



Tweet de desenvolvedor da Ethereum demonstrando sucesso no Shapella Fork na Sepolia.
Fonte: Twitter



Visualização dos slots e épocas logo após o Shapella Fork na rede da Sepolia.
Fonte: sepolia.beaconcha.in/charts/slotviz

Lembrando que o movimento muito parecido ocorreu durante os testes do The Merge no ano passado, no qual a participação pós-fork na Sepolia apresentou a queda para cerca de 70%, algo alarmante mas ainda não problemático. Porém, na atualização da rede principal, observou-se queda desprezível na participação de apenas 3% por um pequeno período.

Isso se dá provavelmente porque, devido ao fato da *mainnet* ter recursos reais, é levada muito mais a sério pelos operadores de nós do que as *testnets* e um resultado similar é esperado para o Shapella Fork na mainnet.

Após este teste bem sucedido, é esperado que em duas semanas - pelo meio de março - se realize o Shapella Fork na rede da Goerli, uma rede de testes mais antiga e *permissionless* da rede da Ethereum, que configurará um *'teste final'* mais robusto para o *fork*.

Por fim, espera-se que duas semanas após o sucesso na Goerli tenhamos, finalmente, a atualização funcional na mainnet da Ethereum, no fim de março ou no início de abril.

Os principais riscos continuam sendo os desconhecidos, mas devido a esta atualização ser bem menos tecnicamente complexa que o The Merge, não é esperado que tenhamos grandes probabilidades de problemas ao executá-la na *mainnet*.

Conclusão

Quanto aos saques, não esperamos venda considerável de etheres após o *fork*, ainda que um cenário agressivo ocorra e essa venda será compensada por novos validadores entrando e *players* que também não participavam do processo devido a iliquidez.

Inicialmente, o preço pode sofrer com a liberação haja vista que a força da narrativa também é considerável, pois muitos investidores que acreditam na grande venda do ativo, se desfazem de suas posições para posteriormente remontá-las a um preço mais favorável.

No longo prazo, porém, acreditamos que o ether tenderá a subir, principalmente devido aos dados econômicos positivos do ativo. Atualmente, observamos uma forte deflação do ether, vindo principalmente do reaquecimento da atividade em DeFi e NFTs, como podemos ver abaixo:

Supply desde o Merge vem caindo consideravelmente,
apresentando comportamento deflacionário para o ether.
Fonte: ultrasound.money

Quanto às outras EIPs inclusas, é muito positivo ver melhorias e otimizações na EVM e em sua estrutura, mas acreditamos que pouco impactarão no preço, e serão mais direcionadas a facilitar o ferramental dos desenvolvedores e criadores de aplicações.

Fontes

Introdução

https://ethereum.org/en/developers/docs/evm/opcodes/
https://notes.ethereum.org/@launchpad/withdrawals-faq
https://ethereum.stackexchange.com/questions/76334/what-is-the-difference-between-bytecode-init-code-deployed-bytecode-creation

Entendendo o fork

https://twitter.com/korpi87/status/1623099650948632576?s=20&t=H94-m9iS61dNs8mV5swJuA
https://messari.io/report/the-withdrawals-are-coming-and-more-ethereum-roadmap-clarity

Shapella Fork
https://blog.ethereum.org/2023/02/21/sepolia-shapella-announcement

Shapella em testnets e Shadow Forks
https://ultrasound.money/
https://twitter.com/terencechain/status/1630426604802555953
https://sepolia.beaconcha.in/charts/slotviz

Disclaimer