O ecossistema de segundas camadas do Ethereum

MB Research

23/08/2022

→ Introdução

O trilema da escalabilidade já assombra os usuários da Ethereum pelo menos desde 2017.
Seu enunciado diz que quando se cria um blockchain, só é possível cobrir efetivamente duas de suas três propriedades relevantes: Descentralização, Segurança e Escalabilidade.

Dado que a segurança é um ponto quase que inegociável e a descentralização é desejada, os blockchains públicos vêm propondo diversas arquiteturas para resolver o problema da escalabilidade, com as mais diversas tecnologias e mecanismos.

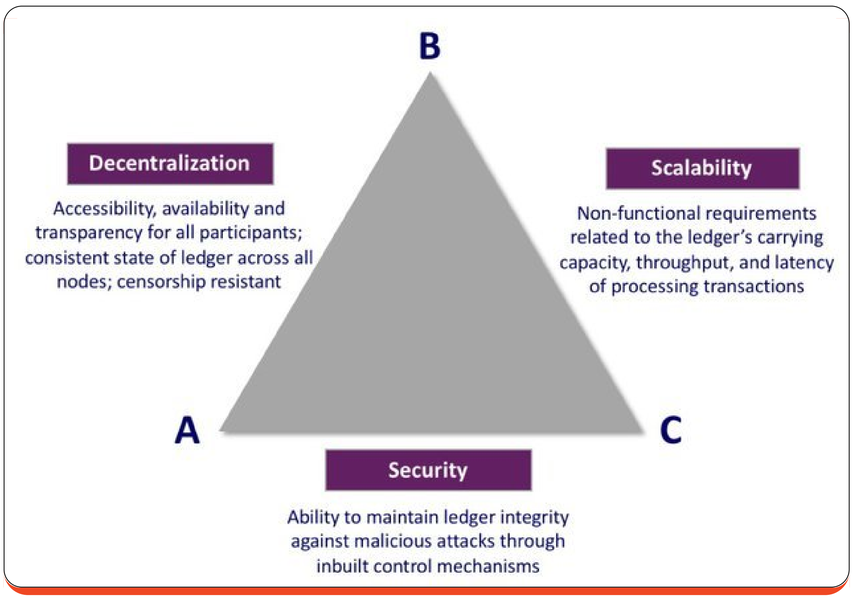


Imagem demonstrativa do trilema da escalabilidade.
Fonte: Research Gate

Hoje em dia, os principais métodos de escalabilidade existentes são:

- **State Channels**
- **Sidechains**
- **Plasma Chains**
- ***Rollups* (Optimistic, Zk, Validiums e Celestiums)**

A tabela comparativa abaixo demonstra os resultados gerais dessas soluções nos principais quesitos de avaliação de escalabilidade:

	State channels	Sidechains[0]	Plasma	Optimistic rollups	Validium	zkRollup
Security						
Liveness assumption (e.g. watch-towers)	Yes	Bonded	Yes	Bonded	No	No
The mass exit assumption	No	No	Yes	No	No	No
Quorum of validators can freeze funds	No	Yes	No	No	Yes	No
Quorum of validators can confiscate funds	No	Yes	No	No	Yes [1]	No
Vulnerability to hot-wallet key exploits	High	High	Moderate	Moderate	High	Immune
Vulnerability to crypto-economic attacks	Moderate	High	Moderate	Moderate	Moderate	Immune
Cryptographic primitives	Standard	Standard	Standard	Standard	New	New
Performance / economics						
Max throughput on ETH 1.0	1..∞ TPS [2]	10k+ TPS	1k..9k TPS [2]	2k TPS [3]	20k+ TPS	2k TPS
Max throughput on ETH 2.0	1..∞ TPS [2]	10k+ TPS	1k..9k TPS [2]	20k+ TPS	20k+ TPS	20k+ TPS
Capital-efficient	No	Yes	Yes	Yes	Yes	Yes
Separate onchain tx to open new account	Yes	No	No	No	No	No [5]
Cost of tx	Very low	Low	Very low	Low	Low	Low
Usability						
Withdrawal time	1 confirm.	1 confirm.	1 week [4] ([7])	1 week [4] ([7])	1..10 min [7]	1..10 min [7]
Time to subjective finality	Instant	N/A (trusted)	1 confirm.	1 confirm.	1..10 min	1..10 min
Client-side verification of subjective finality	Yes	N/A (trusted)	No	No	Yes	Yes
Instant tx confirmations	Full	Bonded	Bonded	Bonded	Bonded	Bonded
Other aspects						
Smart contracts	Limited	Flexible	Limited	Flexible	Flexible	Flexible
EVM-bytecode portable	No	Yes	No	Yes	Yes	Yes
Native privacy options	Limited	No	No	No	Full	Full

[0] Some researchers do not consider them to be part of L2 space at all, see https://twitter.com/gakonst/status/1146793685545304064
[1] Depends on the implementation of the upgrade mechanism, but usually applies.
[2] Complex limitations apply.
[3] To keep compatibility with EVM throughput must be capped at 300 TPS
[4] This parameter is configurable, but most researchers consider 1 or 2 weeks to be secure.
[5] Depends on the implementation. Not needed in zkSync but required in Loopring.
[7] Can be accelerated with liquidity providers but will make the solution capital-inefficient.

Matter Labs

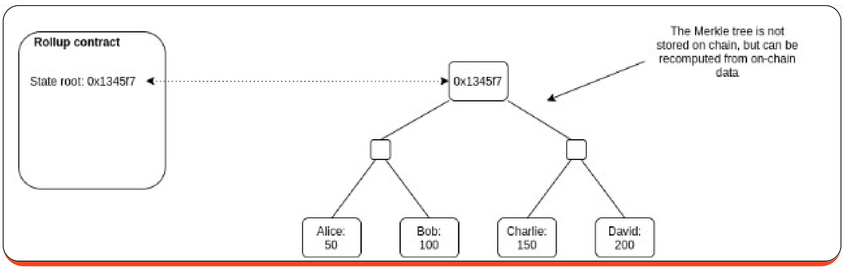
Comparativo entre os principais mecanismos de escalabilidade existentes.
Fonte: Matter Labs

Neste relatório, vamos mergulhar profundamente em diversos mecanismos e aplicações que buscam contribuir para resolver o problema da escalabilidade, discutindo no detalhe seus pontos positivos e negativos.

2. Optimistic rollups

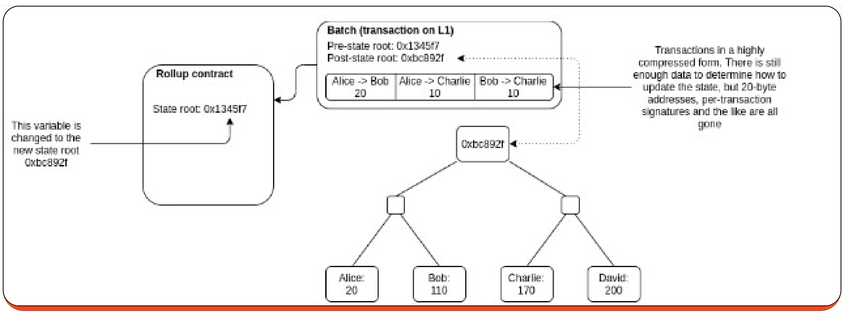
Introdução

Rollups funcionam utilizando um contrato inteligente na *mainnet* do Ethereum, no qual publicam a *Merkle Root* do estado do *rollup*. A *Merkle Root* é uma espécie de 'foto' bem comprimida do estado do *rollup*, isto é, o saldo das carteiras e o código dos contratos dentro do *rollup*, fazendo com que este herde a segurança da rede principal. É importante destacar que a *Merkle Tree*, ou o histórico do estado do *rollup,* não fica armazenado na rede principal, mas pode ser recriado através dos dados *on-chain*.



Esquema de funcionamento de um rollup
Fonte: Vitalik Buterin

A *Merkle Root* no contrato é atualizada quando se realiza uma transação de lote (*batch*), que comprime todas as transações realizadas no *rollup* em uma nova *Merkle Root* e faz referência a última *Merkle Root* como um bloco em uma blockchain.



Esquema de funcionamento de uma transação de lote.
Fonte: Vitalik Buterin

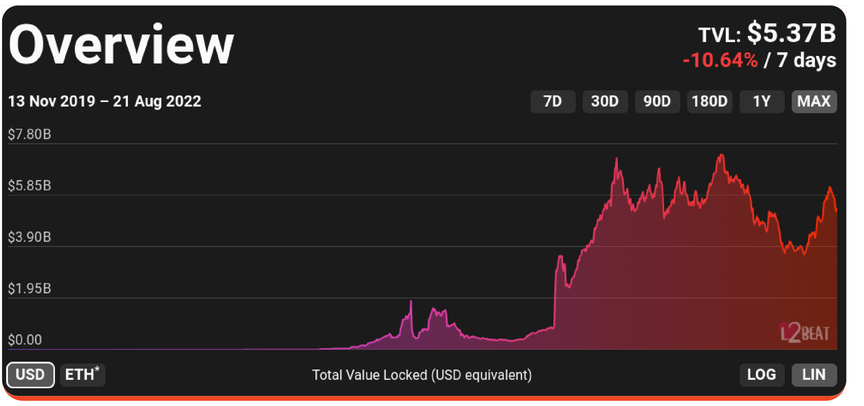
Os contratos inteligentes dos *rollups* também possuem a função de saque e depósito. Para que se possa atualizar o estado da rede, é necessário que se possa incluir transações cujo *input* ou *output* venha de fora do estado do *rollup*. Se uma transação de lote inclui *inputs* de fora do *rollup*, a transação de lote também precisa transferir os ativos depositados ao contrato inteligente do *rollup*. No caso de uma transação de dentro para fora do *rollup*, o contrato, assim que processar a transação de lote, envia os ativos para os endereços que fizeram o saque.

Até o momento, não entramos na maneira em que o contrato inteligente checa a validade da transação de lote, isto porque, existem duas maneiras de fazer esta checagem: os *optimistic rollups* e os *ZK rollups*. Nesta seção, exploraremos a forma que utiliza as provas de fraude, *rollups* que utilizam este método são chamados de *optimistic rollups*, ou *rollups* otimistas.

Rollups otimistas funcionam utilizando provas de fraude. O *rollup* tem um prazo fixo (na maioria das vezes de 7 dias) para a publicar as transações de lote na *mainnet* e, durante este período é possível contestar a *merkle root* computada, produzindo uma prova de fraude que é verificada pelo contrato do *rollup*. Caso a prova de fraude esteja correta, o usuário que elaborou a prova é recompensado e o sequenciador que publicou a transação de lote sofre *slashing*.

A grande vantagem dos *rollups* otimistas é o menor custo de gas ao compor as transações de lote, aproximadamente 40.000 por *batch*, bem menor que os 500.000 necessários por um *ZK rollup*. Além disso, a complexidade técnica necessária para implementar *rollups* otimistas é bem menor do que a de *ZK rollups*, uma vez que os primeiros também apresentam maior facilidade de integração com a EVM, o que facilita a implementação de contratos inteligentes dentro da rede de segunda camada. A grande desvantagem é o longo prazo para efetuar um saque para a rede principal, já que se deve respeitar o prazo necessário para o envio de uma prova de fraude.

A maior facilidade de implementação permitiu que os *rollups* otimistas chegassem primeiro ao mercado, alcançando maior tração em relação a outras soluções de escalabilidade. Hoje, dos US$ 5,37 bilhões em valor total travado em soluções de segunda camada, mais de US$ 4,32 bilhões se encontram em *rollups* otimistas, valor equivalente a mais de 80% do TVL de soluções de segunda camada.



Valor total travado em soluções de segunda camada em dólares americanos.
Fonte: L2 Beat

A seguir exploraremos as particularidades de cada um dos rollups otimistas operacionais no momento.

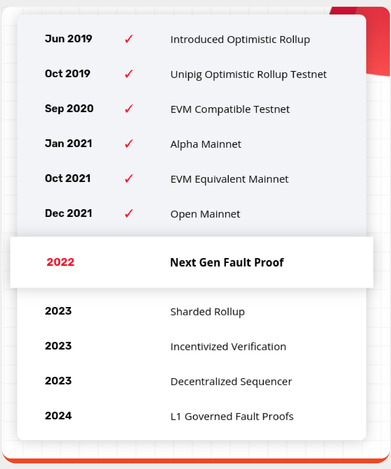
2.1 Optimism

Lançado em 15 de janeiro de 2021, o Optimism foi o primeiro *rollup* operacional do Ethereum. A princípio rodando de maneira permissionada com apenas alguns projetos na rede, a optimism viu pouco uso em seus primeiros meses. Com a atualização no final do ano passado, a rede passou a ser o primeiro *rollup* com equivalência a EVM e passou a permitir a implementação de qualquer contrato inteligente na rede, aumentando o número de Dapps disponíveis para os usuários. No final de maio, o airdrop do token de governança da rede, o OP, causou um crescimento acima do normal no valor total travado, saltando de pouco menos de US$ 1 bilhão, para mais de US$ 1,9 bilhões.

Um diferencial chave da Optimism em relação a seus concorrentes é a equivalência a EVM que a rede possui. De forma simples, isto significa que ao contrário de redes EVM-compatíveis, a Optimism possui conformidade total com o especificado no *Yellow Paper* do Ethereum. Isso é importante, pois garante a portabilidade de contratos inteligentes da *mainnet* para a Optimism sem necessidade de se adaptar o código e o torna completamente compatível com todo o *tooling* existente para o desenvolvimento no Ethereum.

Apesar de já ter dado passos importantes, o projeto ainda está em um estágio inicial, já que ainda não conta com o uso de provas de fraude para garantir a validade das atualizações do estado na *mainnet* e ainda é muito centralizado, contando com um *sequencer* operado pelos desenvolvedores do projeto. O *roadmap* prevê um novo processo para a publicação de provas de fraude previsto para o ano de 2022 e a descentralização do *sequencer* em 2023.

A implementação do processo de publicação de provas de fraude virá junto com uma atualização apelidada de *Bedrock*, em português, algo como alicerce ou fundação. A *Bedrock* trará vários recursos novos para o *rollup* e deverá mudar definitivamente a arquitetura da rede introduzindo maior otimização de custo de gas na publicação de transações de lote. Além disso, também acontecerá a separação entre consenso e execução dentro do *rollup*, tornando-o mais modular e permitindo a implementação de múltiplos clients e mecanismos de prova de fraude que alavancam a descentralização do projeto. Outro fator relevante é que em função do seu design modular a utilização de outras camadas de *data availability*, como os *blobs* propostos pela EIP-4844 (*proto-danksharding*), será extremamente fácil podendo até mesmo ser adaptado para o uso com *ZK rollups*.



Roadmap de desenvolvimento do Optimism.
Fonte: Optimism

Atualmente, a Optimism é a segunda maior segunda camada do Ethereum e conta com US$ 1,61 bilhões de valor total travado.

2.2 Arbitrum

Construído pelo Offchain Labs, o Arbitrum One foi o segundo *rollup* lançado sobre o Ethereum. Iniciado no fim de agosto de 2021, de maneira não permissionada, a Arbitrum One conseguiu tração de maneira muito rápida com seu valor total travado saltando de US$ 111 milhões em 09/09/2021 para mais de US$ 2,6 bilhões em 18/09/2021. O crescimento explosivo pode ser atribuído ao *yield farming* agressivo no protocolo Arbinyan. Hoje, meses após o lançamento do protocolo, o TVL continua alto (US$ 2,68 bilhões) e com uma distribuição muito mais saudável, com a maior parte do capital travada em protocolos de DeFi como GMX, Stargate e Sushiswap.

Neste momento, a Arbitrum One é a maior solução de escalabilidade do Ethereum em valor total travado. Seu sucesso, com certeza, pode ser atribuído ao modelo não permissionado do lançamento, que permitiu que em questão de semanas várias aplicações fossem implementadas na rede.

Em 11 de outubro de 2021, a Offchain Labs revelou o Arbitrum Nitro, a próxima iteração do projeto. O Nitro terá como base o Geth, cliente mais utilizado do Ethereum, e WASM permitindo transações ainda mais rápidas e baratas, além de melhorar a compatibilidade do código utilizado em contratos inteligentes na rede com a EVM. A rede da Arbitrum One será atualizada com o Nitro sem nenhum tipo de atrito, atualmente em fase de testes, a atualização está prevista para 31 de agosto de 2022.

A Arbitrum está em estágios iniciais de desenvolvimento e também possui problemas de centralização. Atualmente apenas endereços em uma *whitelist* podem enviar provas de fraude ao contrato da Arbitrum na *mainnet* e o *sequencer* é centralizado.

2.3 Boba network

O Boba Network é um *fork* da Optimism desenvolvido pela Enya, um dos times contribuidores da OMG Foundation. O Boba network se diferencia do optimism devido a recursos únicos como o saque rápido da rede (muito menos dos 7 dias necessários na Optimism) e a lógica de definição do preço das taxas de rede.

Atualmente, a rede conta com pouco menos de US$ 36 milhões em valor total travado, uma queda significativa em relação à máxima de US$ 1,38 bilhões em novembro de 2021.

Por ser um *fork* da Optimism, o Boba Network também herdou todos os problemas de centralização presentes no projeto original.

2.5 Layer2.finance

A Layer2.finance é um *rollup* otimista desenvolvido pela Celer Network que tem uma proposta diferente dos demais. Ao invés de criar um ecossistema DeFi dentro do *rollup*, a Layer2.finance utiliza o ecossistema DeFi existente através da Celer cBridge. Hoje, a Layer2.finance permite a utilização da Aave, Compound e Curve através de sua rede.

Apesar da proposta interessante, a rede não tem muita utilização, já que conta com apenas US$ 188 mil em valor total travado, um valor desprezível em comparação com até mesmo protocolos DeFi dentro do Ethereum.

2.6 Fuel V1

A Fuel v1 também é um *rollup* otimista que apresenta algumas diferenças chave em relação às demais soluções de escalabilidade do Ethereum, isto porque, a rede utiliza o modelo de UTXO, assim como o bitcoin e uma linguagem de programação única, o Sway.

O modelo de UTXO permite que transações sejam processadas em paralelo, trazendo uma melhoria significativa na escalabilidade em relação ao modelo baseado em contas utilizado pelo Ethereum e a grande maioria dos *rollups*.
A Fuel também resgata a ideia de moedas "coloridas" para o uso com ETH e qualquer token ERC-20.

Devido a arquitetura do modelo de transação na Fuel, também é possível construir Exchanges não custodiais dentro da rede e realizar *swaps* atômicos *cross-chain* para saques instantâneos do *rollup*, atualmente a rede permite swaps atômicos com a rede do Bitcoin, Cosmos e Polkadot. Além disso, o esquema de prova de fraude utilizado na Fuel é diferente devido a sua arquitetura, permitindo maior economia na atualização do estado da rede na *mainnet*.

Apesar da tecnologia revolucionária, o *rollup* tem baixíssima adesão com apenas US$ 8 em valor total travado. A baixa adesão pode ser explicada por alguns fatores, como a complexidade de desenvolvimento na rede e o envolvimento dos desenvolvedores com outros projetos, como a Celestia.

3. ZK-rollups

Introdução

Assim como todos os outros, os *Zero Knowledge rollups* são uma família de *rollups* que visa aumentar a escalabilidade por meio do empacotamento de diversas transações em um único pacote, que deve ser retornado para a cadeia principal. Sua grande especialidade é o uso de 'provas de conhecimento zero', para tal, vamos explorar exemplos desse conceito.

Uma **prova de conhecimento zero** é um método criptográfico no qual o provador consegue provar ao verificador que certa informação é válida, sem que haja transmissão da informação em si e de nenhuma outra informação extra.

Na verdade, os *Zk-proofs* são baseados em probabilidades e estatística, como vamos demonstrar no exemplo abaixo, uma versão adaptada do livro "How to explain Zero-Knowledge Proof to your children', de Jean-Jacques Quisquater.

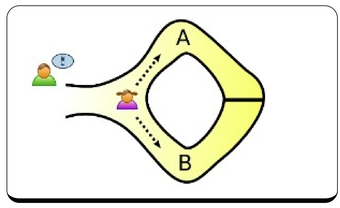
Exemplo

Suponha que exista uma caverna e,nessa caverna, exista uma porta de diamantes que só pode ser aberta com uma única chave existente.

Imagine que duas pessoas (Provador e Verificador) estejam inicialmente juntas do lado de fora dessa caverna.

O Provador quer provar ao Verificador que possui a chave para abrir a porta, sem efetivamente mostrar ao verificador que possui a chave (configurando uma prova de conhecimento zero).

Para tal, eles nomeiam os caminhos possíveis na caverna de A e B, conforme visto abaixo:



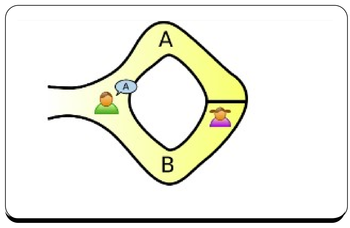
O provador, então, entra na caverna e escolhe um dos dois caminhos possíveis.
Repare que o verificador não sabe qual caminho ele escolherá.

Em seguida, o Verificador entra na caverna e joga uma moeda, que indicará por qual lado o Provador terá que regressar:

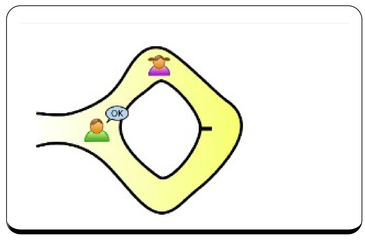
Cara → regressar pelo lado A

Coroa → regressar pelo lado B

Declarando o resultado em voz alta para que o Provador ouça.



Por fim, o Provador regressa pelo caminho necessário, terminando a primeira iteração do mecanismo.



Caso o Provador não consiga regressar pelo caminho solicitado, a prova será automaticamente negada.

Caso contrário, vamos entender os possíveis cenários vencedores desse mecanismo:

Validador/Provador	A	B
A	Não é necessária chave	É necessária chave
B	É necessária chave	Não é necessária chave

Percebemos que, simplesmente ao acaso, metade dos resultados não necessitam da posse da chave para serem validados, já que 50% de certeza não é um limite aceitável para considerar a prova como válida. Para aumentar essa probabilidade, esse processo terá que ser repetido *n* vezes.

A cada iteração executada com sucesso, a probabilidade do Validador ter sucesso em todos os resultados ao acaso vai ficando cada vez menor, seguindo a fórmula: 1/2n.

Interação	1	2	3	4	5	6	7	8	9	10
Probabilidade de caso	50%	25%	12,5%	6,25%	3,12%	1,56%	0,78%	0,39%	0,19%	0,1%

Interação	11	12	13	14	15	16	17	18	19	20
Probabilidade de caso	0,05%	0,02%	0,01%	60ppm	30ppm	15ppm	7,5ppm	3,75ppm	1,9ppm	0,9ppm

O que resulta em menos de uma chance em um milhão, na vigésima iteração. Pode-se, porém, seguir o procedimento indefinidamente, reduzindo a confiança necessária a cada etapa até valores arbitrariamente baixos.
A prova de conhecimento zero é então aceita, quando essa probabilidade for menor que um valor arbitrário *k*, aceito como a margem mínima de confiança.

O que compõe uma prova de conhecimento zero

Devido à natureza probabilística (não-determinística) das provas de conhecimento zero, é necessário cautela na definição de seus pré-requisitos e termos.

Provas de conhecimento zero, principalmente as com poucas iterações, podem ter um *erro de corretude* alto, sendo necessário grande número de iterações para minimizá-lo. **Nunca** é possível garantir que ele será efetivamente zero, devido a natureza probabilística já mencionada.

O termo '*eventualmente*' quando usado nas definições a seguir, significa o **limite quando o número de iterações tende ao infinito,** que pode ser entendido, em outros termos, como o limite de quando o *erro de corretude* tende a zero.

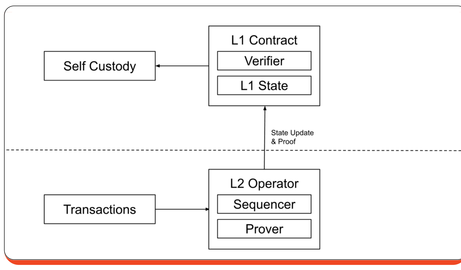
A definição de '*honestidade*' também é relevante, trata-se de um participante (Verificador ou Provador) que **segue estritamente as regras do protocolo** de conhecimento zero.

Dado o *disclaimer* acima, vamos à definição.

Uma prova de conhecimento válida deve atender a três propriedades:

- **Integralidade/Completude:** caso a afirmação seja verdadeira, um Verificador honesto será *eventualmente* convencido da mesma forma por um Provador honesto.
- **Solidez/Corretude:** caso a afirmação seja falsa, um Provador desonesto não conseguirá (nem *eventualmente*) convencer um Verificador honesto de que ela é verdadeira.
- **Conhecimento Zero:** dado que a afirmação é verdadeira, um Provador honesto *eventualmente* conseguirá garantir sua veracidade ao Verificador honesto, sem que esse obtenha qualquer tipo de informação adicional sobre a mesma.

Caso o leitor tenha interesse na prova matemática rigorosa, é possível consultá-la (em inglês) no seguinte endereço: https://crypto.stanford.edu/pbc/notes/crypto/zk.html



Modelo simplificado da arquitetura transacional de um *Zk-rollup*.
Fonte: Medium ImmutableX

Possíveis Métodos de uma prova de conhecimento zero

Existem também duas classificações de provas de conhecimento zero, as **ZK-SNARKs** e as **ZK-STARKs.**

Zk-STARK é um acrônimo para **z**ero-**k**nowledge **s**calable **t**ransparent **ar**gument of **k**nowledge, enquanto as zk-SNARKs são **z**ero-**k**nowledge **s**uccint **n**on-interactive **ar**guments of **k**nowledge. Ou seja, a diferença entre esses dois mecanismos é o **método** que eles usam para provar seu conhecimento.

SNARKS

SNARKS nasceram em 2012 e são dependentes da criptografia de curva elíptica para executar suas provas. Estas são vulneráveis a computadores quânticos e também dependem de um *setup* confiável, ou seja, do evento da primeira criação de chaves a serem usadas para realizar as provas necessárias e suas verificações.

Os dados utilizados para criar essas chaves devem ser prontamente destruídos após seu uso, pois a utilização indevida de tal informação quebraria o sistema de provas do método. O lado positivo, é que isso deve ser realizado apenas uma vez, no início do protocolo.

Levando todos esses pontos em consideração, a adoção do mecanismo SNARK é mais ampla do que sua contraparte, pois foi desenvolvido antes do mecanismo STARK e possui bibliotecas de desenvolvimento mais amplas e acessíveis, além de mais suporte.
Outros pontos positivos deste método, são que ele gasta consideravelmente menos *gas* do que o outro mecanismo (cerca de 24% do que consome o STARK), tendo como consequência transações mais baratas para o usuário final e a menor necessidade de espaço de armazenamento para suas provas, o que significa uma menor necessidade de armazenamento de dados *on-chain*.

STARKS

O primeiro paper descrevendo o método foi escrito em 2018, o que evidencia como é recente essa tecnologia. Ela se baseia não em curvas elípticas, mas em funções de hash, sendo um de seus principais benefícios uma consequência dessa escolha, que faz com que eles sejam resistentes à computação quântica. Além disso, usar um método STARK não necessita do *setup* confiável, reduzindo ainda mais o risco de problemas futuros no protocolo.

Os pontos negativos são quase que complementares aos discutidos na seção dos SNARKs: a escassez de documentação e suporte de bibliotecas do método e os tamanhos das provas consideravelmente maiores que podem se tornar pedras no caminho da evolução desse método.

A Ethereum Foundation e outras instituições estão incentivando o desenvolvimento de soluções para os problemas observados no método STARK, já que o enxergam como mais promissor a longo prazo do que a sua contraparte. Recentemente, a EF deu à STARKware uma bolsa de US$ 12 milhões para o desenvolvimento de seus produtos.

BULLETPROOFS

Existe ainda um terceiro método, conhecido como ***Bulletproof***, desenvolvido também entre 2017 e 2018, por um grupo de cientistas de Stanford. O método busca se beneficiar das características positivas de ambos métodos SNARK e STARK, já que não necessitam de *setups* iniciais confiáveis para sua criação, assim como os STARKs, mas também contam com o benefício de não necessitar de provas gigantescas, assim como os SNARKs.

Tecnologias do método Bulletproof já foram implementadas com sucesso no criptoativo focado em privacidade Monero e, desde então, seus resultados estão sendo avaliados como um meio termo entre os dois métodos mais consagrados.

Mais estudos, testes e experimentos são necessários para garantir sua superioridade, mas os resultados iniciais do método dão indício de serem promissores.
Existe ainda um terceiro método, conhecido como Bulletproof, desenvolvido também entre 2017 e 2018, por um grupo de cientistas de Stanford. O método busca se beneficiar das características positivas de ambos métodos SNARK e STARK, já que não necessitam de setups iniciais confiáveis para sua criação, assim como os STARKs, mas também contam com o benefício de não necessitar de provas gigantescas, assim como os SNARKs.

Tecnologias do método Bulletproof já foram implementadas com sucesso no criptoativo focado em privacidade Monero e, desde então, seus resultados estão sendo avaliados como um meio termo entre os dois métodos mais consagrados.

Mais estudos, testes e experimentos são necessários para garantir sua superioridade, mas os resultados iniciais do método dão indício de serem promissores.

	SNARKs	STARKs	Bulletproofs
Algoritmic complexity: prover	O(N * log(N))	O(N * poly-log(N))	O(N * log(N))
Algoritmic complexity: verifier	~O(1)	O(poly-log(N))	O(N)
Communication complexity (proof size)	~O(1)	O(poly-log(N))	O(log(N))
- size estimate for 1 TX	Tx: 200 bytes, Key: 50 MB	45 kB	1.5 kb
- size estimate for 10.000 TX	Tx: 200 bytes, Key: 500 GB	135 kb	2.5 kb
Ethereum/EVM verification gas cost	~600k (Groth16)	~2.5M (estimate, no impl.)	N/A
Trusted setup required?	YES 😒	NO 😀	NO 😀
Post-quantum secure	NO 😒	YES 😀	NO 😒
Crypto assumptions	Strong 😒	Collision resistant hashes 😀	Discrete log 😒

Comparação técnica entre os principais métodos de *rollup* de conhecimento zero
Fonte: consensys.net/blog/blockchain-explained/zero-knowledge-proofs-starks-vs-snarks/

Mais informações acerca desses métodos podem ser encontradas no seguinte recurso e outros descritos na seção de fontes deste relatório:

https://ethereum.org/pt/developers/docs/scaling/zk-rollups/

Dada a explicação, vamos analisar exemplos de aplicações que se utilizam desta tecnologia.

3.1 Loopring

O Loopring é um protocolo de ZK *Rollup* baseado na Ethereum, lançado em junho de 2017 pela Loopring Foundation.
Seu principal líder é Daniel Wang, engenheiro de software Chinês e seu foco principal são os pagamentos e *swaps on chain*.
O *rollup* possui sua moeda nativa, o LRC, cujo *token economics* pode ser visto aqui e é governado pela LoopringDAO.

Segundo o *l2beat.com*, site que avalia a performance de diversos layer2, o *rollup* possui atualmente um valor travado (TVL) de aproximadamente US$214 milhões, sendo aproximadamente ⅔ desse volume correspondente aos próprios tokens LRC. Ainda assim, a aplicação só possui cerca de 3,5% do *market share* total, configurando em segundo lugar entre os *rollups* de ZK e 4º no quadro geral.

O protocolo usa a tecnologia de ZK-Snarks e, no momento de uma transação de envio de *etheres* por meio do mesmo, custa US$0,02, enquanto um *swap* custa US$ 0,39.

3.2 ZkSync

O ZkSync é um dos protocolos mais promissores no segmento de *rollups* de conhecimento zero. Recentemente, os desenvolvedores anunciaram o lançamento de uma versão 2.0 do protocolo (zkEVM) a ser entregue em cerca de 3 meses, que promete ser EVM-compatível. Esse fato envolve grande complexidade técnica e tem forte potencial de revolucionar o mercado.

O projeto ainda não possui token próprio, mas tem o projeto de lançá-lo no futuro. Seus principais parceiros são a Ethereum Foundation, Dekrypt Capital e a Dragonfly Capital.

É desenvolvido e mantido pelo MatterLabs, empresa sediada em Berlim, na Alemanha, mas seus colaboradores estão espalhados pela Europa e pelo mundo.

Segundo o *l2beat.com*, atualmente, o *rollup* possui um valor travado (TVL) de aproximadamente US$71 milhões. A aplicação só possui cerca de 1,2% do *market share* total, configurando em terceiro lugar entre os *rollups* de ZK e 6º no quadro geral.

O protocolo usa a tecnologia de ZK-Snarks e, no momento, uma transação de envio de *etheres* por meio do mesmo custa US$0,03, enquanto um swap custa US$ 0,07.

3.3 ZkSwap e ZkSpace

Nos dias de hoje, o ZkSwap possui três versões de seu protocolo, a v1 e a v2, antigas, mas que ainda se encontram em uso, e também uma nova versão v3, que é conhecida como ZkSpace. O projeto nasceu como um *fork* do ZKSync, com a adição de funcionalidades de suporte a AMMs e NFTs.

Segundo o *l2beat.com*, atualmente, o ZkSpace possui um valor travado (TVL) de aproximadamente US$53 milhões. A aplicação só possui cerca de 0,9% do *market share* total, configurando em quarto lugar entre os *rollups* de ZK e 8º no quadro geral.

Suas duas versões anteriores somadas (ZkSwap 1.0 e 2.0) possuem valor travado de US$ 2,5 milhões, valor vinte vezes menor do que a atual implementação.
O protocolo usa a tecnologia de ZK-Snarks e já possui um token próprio, o ZKS.

3.4 Aztec Connect

A Aztec é um ZK-rollup que tem como principal objetivo fornecer privacidade nas transações de seus usuários em DeFi.
Seu sistema de transações é análogo ao do Bitcoin, utilizando-se do modelo de UTXO.
O protocolo usa a tecnologia de ZK-Snarks e ainda não possui token próprio, mas dá indícios que pretende lançá-lo quando o produto atingir a maturidade.
Segundo o *l2beat.com*, atualmente, o *rollup* possui um valor travado (TVL) de aproximadamente US$7,6 milhões. A aplicação só possui cerca de 0,1% do *market share* total, configurando em quinto lugar entre os *rollups* de ZK e 12º no quadro geral.

Uma versão antiga do protocolo (apenas Aztec) também está registrada, com um TVL de aproximadamente US$5 milhões, ainda um dos menores valores entre os *rollups*, mesmo que somados.

Segundo o *l2fees.info*, no momento, uma transação de envio de *etheres* por meio do mesmo custa US$0,39.

3.5 Polygon Hermez/ zkEVM

Polygon Hermez ou zkEVM é a investida da Polygon em ZK-rollups.
O projeto Hermez já existia anteriormente, com seu token HEZ, mas parte do acordo de compra pela Polygon, em agosto de 2021, envolveu a fusão deste token com o próprio MATIC, nativo da Polygon.

Modelo de escalabilidade da Polygon Hermez/zkEVM
Fonte: blog.polygon.technology

Segundo o *l2beat.com*, atualmente, o rollup possui um valor travado (TVL) de aproximadamente US$0,4 milhões. A aplicação só possui cerca de 0,01% do *market share* total, configurando em último lugar entre os rollups de ZK e 19º no quadro geral.

Segundo o *l2fees.info*, no momento, uma transação de envio de *etheres* por meio do mesmo custa US$0,25.

3.6 StarkNet e StarkEx

A StarkNet é um *rollup* Zk-Stark que usa a engine de escalabilidade da StarkEx. Essa *engine* também é utilizada em outros projetos, principalmente em Validiums, como Sorare, dYdX, ImmutableX, rhino.fi e Celer.

Segundo o *l2beat.com*, atualmente, o StarkNet possui um valor travado (TVL) de aproximadamente US$1,4 milhões. A aplicação só possui cerca de 0,02% do market share total, configurando em sétimo lugar entre os *rollups* de ZK e 17º no quadro geral.

Como abordaremos na seção a seguir, porém, o uso da StarkEx por diversos Validiums possui TVL de mais de meio bilhão de dólares, mostrando a força dessa *engine*.

3.7 dYdX

A dYdX é uma das maiores DEX do mercado cripto.
Com forte foco em derivativos e perpétuos, o protocolo observou grande crescimento no volume de transações nos últimos meses.

Lançado em novembro de 2020, o promissor projeto conta com diversos fundos de *Venture Capital* por trás de sua expansão.
O lançamento do token, em agosto de 2021, e o TVL recorde de cerca de 800k ETH atingido em julho de 2022, foram os principais marcos para o protocolo que acumula centenas de usuários e cada vez mais recordes.

Evolução do TVL do dYdX em etheres.
Fonte: Defi Llama

A dYdX possui atualmente TVL de US$ 485 milhões, configurando em terceiro lugar entre os maiores *rollups*, perdendo apenas para os otimistas Arbitrum e Optimism.

4. Validiums

Introdução e Definições

Validiums são um tipo de solução de escalabilidade que se utiliza da tecnologia dos Zk-proofs, mas diferentemente destas, não registram o resultado das transações nas chains principais.

	SNARKs/ STARKs	Fraud proofs
Data on-chain	ZK rollup	Optimistic rollup
Data off-chain	Validium	Plasma

Classificação dos mecanismos de escalabilidade conforme método e armazenamento de dados utilizado.VM
Fonte: Eli Ben Sasson e Vitalik Buteri

Esses protocolos usam dados *off-chain*, ou seja, fora do blockchain, para armazenar as provas das transações, podendo ser do tipo Zk-SNARKs ou Zk-STARKs. Essa separação de responsabilidades favorece a alta velocidade e as baixas taxas nas transações, mas o *trade-off* é uma segurança que depende do modelo de armazenamento *off-chain (data availability)* utilizado.

O armazenamento *off-chain* introduz certo grau de centralização aos protocolos que decidem utilizá-lo. A StarkEx, por exemplo, principal engine utilizada atualmente pelos Validiums, possui o Data Availability Committee (DAC), um comitê composto de oito organizações que é responsável pelo cálculo e verificação de dados com a rede principal, e não pode validar nenhum estado isoladamente, sem que os oitos membros estejam de acordo.

É evidente que esse mecanismo ainda será significativamente menos seguro do que a maioria dos blockchains públicos. Em teoria, um único membro do DAC ainda pode congelar os fundos dos usuários. Além disso, atualmente, é difícil garantir que essas organizações conhecidas responsáveis pela segurança de todo o sistema StarkEx nunca estarão um dia sujeitas à pressão regulatória para realizar o KYC dos usuários ou até mesmo ajudar as agências regulatórias a congelar os fundos dos usuários.

4.1 Immutable X

Immutable X é um Validium que utiliza a StarkEx para processamento de transações com armazenamento de dados off-chain. Seu principal foco são *games* e coleções de NFTs e, entre seus usuários notáveis estão, Illuvium, Disney, Gods Unchained, Marvel, Ember Sword, entre outros.

O Immutable X foi fundado por James Ferguson, empresário que anteriormente liderou equipes de desenvolvimento de software junto ao seu irmão Robbie Ferguson.

Atualmente, a equipe é composta por mais de 100 membros com diferentes *backgrounds* e os principais investidores do projeto são figuras importantes do mundo blockchain, como Coinbase, Naspers, Nirvana Capital, Apex Capital Partners, Continue Capital e Galaxy Digital.

O projeto possui token próprio, o IMX, que foi lançado em novembro de 2021 e a Immutable X, atualmente, possui TVL de US$ 52 milhões, configurando em sétimo lugar entre os maiores *rollups*, sendo o segundo maior Validium.

4.2 DeversiFi/ Rhino.fi

A atual rhino.fi (antigamente conhecida como Deversi.fi) também é uma solução que utiliza Validium com suporte do StarkEx. Seu principal foco é promover um ambiente DeFi integrado e *multi-chain* para seus usuários.

O projeto possui o token de governança DVF, herança de seu antigo nome. Entre seus principais parceiros podemos destacar a Delphi Ventures, Consensys, Bitfinex e a Parafi Capital.

Atualmente, a rhino.fi possui TVL de US$ 24,6 milhões, configurando em décimo primeiro lugar entre os maiores *rollups,* sendo o quarto maior Validium.

4.3 Sorare

A Sorare é um game *free-to-play* de NFTs, com funcionalidades de exchange, que se utiliza também da *engine* do StarkEx para desenvolver um game que mistura colecionáveis e desempenho de atletas no mundo real *(fantasy sports)*.Atualmente, o projeto conta com jogadores de mais de 280 clubes de futebol mundiais e a liga americana de baseball.

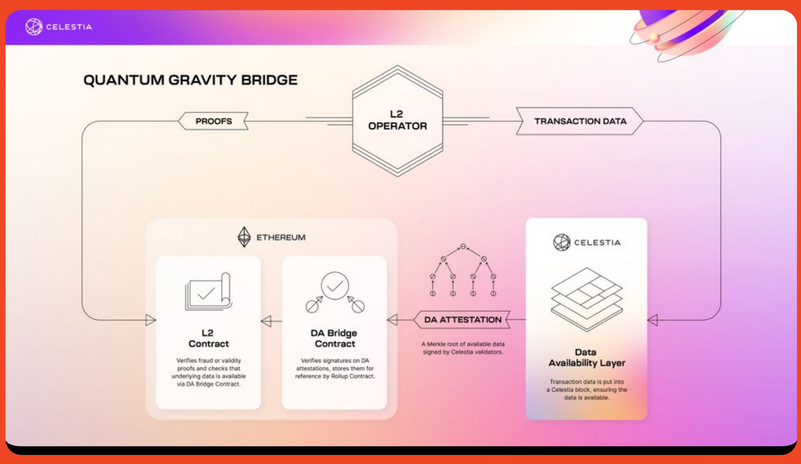
Neste momento, a Sorare possui TVL de US$ 26,3 milhões, configurando em décimo lugar entre os maiores *rollups*, sendo o terceiro maior Validium.

O projeto ainda não possui seu token próprio.

5. Celestiums

Celestiums se assemelham a Validiums, porém com uma diferença chave que, ao invés dos dados de transação serem postados em um banco de dados centralizados, ela se utiliza do blockchain da Celestia como uma camada de disponibilidade de dados para o armazenamento destas informações, o que torna seu processo mais descentralizado e seguro.

Celestiums utilizam o Ethereum como camada de consenso e a Celestia como uma camada de disponibilidade de dados. O uso da Celestia, como camada de disponibilidade de dados, se faz possível utilizando a Quantum Gravity Bridge, que permite que o contrato do celestium no Ethereum consiga atestar que os dados estão disponíveis no blockchain da Celestia.



Esquema de funcionamento de um Celestium
Fonte: Celestia

Como se deve pagar mais taxas utilizando este método, Celestiums devem ter taxas mais altas que Validiums mas, em contrapartida, oferecem maior segurança. Como a Celestia utilizará o Tendermint como mecanismo de consenso, qualquer falha na disponibilidade dos dados do Celestium pode ser penalizada com *slashing*, o que garante uma segurança criptoeconômica a solução de escalabilidade.

Como a Celestia ainda está em fase de testes, não existem Celestiums em operação.

6. Conclusão

Nos dias atuais, a escalabilidade é o maior obstáculo para a ampla adoção do Ethereum, uma vez que, soluções de segunda camada podem oferecer escalabilidade a seus usuários que aproveitam a segurança e descentralização presente na rede principal. Apesar de ainda em estágio inicial, os *rollups* já concentram parte considerável da atividade *on-chain* e, com o *roadmap* do Ethereum pendendo para uma solução *rollup*-cêntrica, poderemos ver essa atividade crescer ainda mais nos próximos meses.

Name	Send ETH	Swap tokens
Loopring	$0.02	$0.39
ZKSync	$0.03	$0.07
Arbitrum One	$0.09	$0.14
Optimism	$0.09	$0.13
Boba Network	$0.09	$0.24
Polygon Hermez	$0.25	-
Aztec Network	$0.39	-
Ethereum	$0.53	$2.64

Os *rollups* que estão hoje em operação alcançaram o objetivo de oferecer maior escalabilidade para seus usuários com um maior número de transações por segundo e taxas mais baixas, entretanto, como vimos ao longo deste relatório, grande parte destes projetos precisam melhorar sua descentralização para que possam, de fato, oferecer uma experiência semelhante a *mainnet.*

Projetos como Optimism e Arbitrum já contém em seus respectivos *roadmaps* atualizações para chegar no objetivo de uma solução de segunda camada completamente descentralizada. Projetos de zk-rollups evoluem também em velocidades rápidas, com entregas como a da ZKSync sendo prometidas antes mesmo do final deste ano.

Com a implementação da EIP-4844 e outras EIPs que visam promover a escalabilidade, no Shanghai Fork (provavelmente na primeira metade de 2023), as taxas de transação em *rollups* deverão ficar ainda mais baratas e impulsionar a adoção deste tipo de solução.

O futuro do Ethereum está intimamente relacionado à evolução das soluções de segunda camada, por isso, é importante acompanhar o desenvolvimento desta tecnologia. A relação simbiótica entre o Ethereum e seu ecossistema de *rollups* é o ponto chave na visão de desenvolvimento modular do protocolo.

7. Fontes

Optimism:
https://l2beat.com/projects/optimism/
https://community.optimism.io/docs/protocol/
https://www.optimism.io/about
https://medium.com/ethereum-optimism/introducing-evm-equivalence-5c2021deb306
https://www.youtube.com/watch?v=wTsmYKfTVIg

Arbitrum:
https://developer.offchainlabs.com/docs/Mainnet
https://github.com/OffchainLabs/nitro
https://offchain.medium.com/mainnet-for-everyone-27ce0f67c85e
https://medium.com/offchainlabs/arbitrum-nitro-sneak-preview-44550d9054f5

Boba Network:
https://docs.boba.network/
https://l2beat.com/projects/bobanetwork/

Layer2.finance:
https://l2beat.com/projects/layer2finance/
https://blog.celer.network/2021/04/22/the-layer2-finance-v0-1-mainnet-launches-democratize-defi-simple-and-zero-fees/
https://docs.l2.finance/#/

Fuel v1:
https://l2beat.com/projects/fuelv1/
https://docs.fuel.sh/v1.1.0/Introduction/Welcome.html
https://fuellabs.github.io/sway/v0.20.2/
https://en.bitcoin.it/wiki/Colored_Coins

ZK-rollups:
Introdução, Exemplo e Definições
https://docs.ethhub.io/ethereum-roadmap/layer-2-scaling/zk-rollups
https://pages.cs.wisc.edu/~mkowalcz/628.pdf
https://ethereum.org/pt/developers/docs/scaling/zk-rollups/
https://members.delphidigital.io/reports/the-complete-guide-to-rollups
https://crypto.stanford.edu/pbc/notes/crypto/zk.html
https://immutablex.medium.com/ground-up-guide-zkevm-evm-compatibility-rollups-787b6e88108e
https://l2beat.com/
https://l2fees.info/
https://eprint.iacr.org/2018/046.pdf
https://consensys.net/blog/blockchain-explained/zero-knowledge-proofs-starks-vs-snarks/
https://moneymade.io/learn/article/zk-rollups-explained
https://offshift.io/public/blog/2021-11-24-bulletproofs-zksnarks-zkstarks

Loopring:
https://loopring.org/#/lrc,
https://medium.loopring.io/lrc-tokenomics-v2-1e6fd99e9e9c ,

ZkSync:
zksync.io
https://blog.matter-labs.io/zksync-2-0-public-testnet-is-live-de870ba9632a
https://matter-labs.io/
https://matterlabs.notion.site/Matter-Labs-Team-Handbook-43342b471fe14f05b2baf250cb7c7a02

ZkSpace e ZkSwap:
zks.org

Aztec Network:
https://aztec.network/

Polygon Hermez/ zkEVM:
https://polygon.technology/solutions/polygon-zkevm/
https://blog.polygon.technology/the-future-is-now-for-ethereum-scaling-introducing-polygon-zkevm/

StarkNet e StarkEx:
https://l2beat.com/projects/starknet/
https://star kware.co/starkex/

dYdX:
https://defillama.com/protocol/dydx?denomination=ETH

Validium:
Introdução e Definições
https://ethereum.org/en/developers/docs/scaling/validium/
https://min.news/en/economy/
https://medium.com/starkware/hello-cairo-3cb43b13b209

ImmutableX:
https://immutablex.medium.com/ground-up-guide-zkevm-evm-compatibility-rollups-787b6e88108e
https://coinmarketcap.com/pt-br/currencies/immutable-x

DiversiFi/ rhino.fi:
https://coinmarketcap.com/pt-br/currencies/deversifi/
https://rhino.fi/

Sorare:
https://l2beat.com/projects/sorare/

Celestium:
https://blog.celestia.org/celestiums/

Nossos especialistas

André Franco

André é Engenheiro Mecatrônico e Analista de criptoativos desde 2017, foi eleito uma das 50 maiores personalidades cripto do Brasil pelo Cointelegraph, com vasta experiência no mercado, André é atualmente o diretor de Research do Mercado Bitcoin.

Rony Szuster

Rony é Engenheiro Químico com pós-graduação em Engenharia de Software, imerso no mercado cripto desde 2019 e analista contribuidor da Messari desde 2021. Atualmente integra a equipe de analistas de criptoativos da Mercado Bitcoin.

Lucca Benedetti

Lucca é estudante de Engenharia Química e um entusiasta do mercado desde 2015, se tornou analista de forma profissional em 2021 com experiência no nascente campo de finanças descentralizadas (DeFi). Atualmente integra a equipe de analistas de criptoativos no Mercado Bitcoin.

Bernard Pedra

Bernard é estudante de blockchain e criptografia digital e entusiasta do mercado desde 2019 com experiência prática no campo de tokens-não-fungíveis (NFT). Atualmente integra a equipe de analistas de criptoativos no Mercado Bitcoin.

Disclaimer

Este relatório foi elaborado e distribuído pelo Mercado Bitcoin Serviços Digitais Ltda. ("Mercado Bitcoin").

Este documento tem como objetivo informar os investidores de criptoativos, não constituindo e nem devendo ser interpretado como sendo uma oferta de compra ou de venda dos criptoativos contidos neste relatório.

Esse relatório não indica qualquer retorno garantido e as decisões de investimentos devem ser realizadas pelo próprio investidor. Este material foi elaborado de forma independente, e a cópia, reprodução e distribuição deste conteúdo - integral ou parcialmente - só pode ser realizada com prévia autorização expressa do Mercado Bitcoin.

Embora tenham sido tomadas todas as medidas razoáveis para assegurar que as informações aqui contidas não são incertas ou equívocas no momento de sua publicação, uma vez que o relatório tomou como base informações públicas de fontes consideradas confiáveis, o Mercado Bitcoin e os seus analistas não respondem por eventuais inexatidões, omissões ou erros das informações do conteúdo.

MB Research

Mercado Bitcoin