NBIT11

O próximo capítulo da gestão de portfólios já começou

- O Bitcoin surgiu como resposta à crise de 2008, trazendo um sistema monetário digital e descentralizado.
- O Índice Sharpe aumenta em mais de 30%, ao adicionar apenas 1% de Bitcoin a um tradicional portfólio 60-40.
- O NBIT11 oferece exposição sintética via futuros da B3, eliminando riscos da autocustódia.

Uma nova espécie monetária

Na natureza, linhagens descendentes herdam características de seus ancestrais, variações ocorrem de tempos em tempos, e a adaptação é condição indispensável para a perpetuação e sobrevivência. O início de uma nova espécie é marcado por poucos indivíduos, às vezes frágeis. Mas o tempo é implacável, e a seleção natural cumpre seu papel: os organismos mais adaptados persistem, enquanto os que não se adaptam desaparecem.

Em 2008, em meio à grande crise financeira e em busca de alternativas ao sistema financeiro tradicional, Satoshi Nakamoto dá início a uma nova forma de dinheiro. Algo como uma nova espécie, num ambiente dominado por entidades já estabelecidas: títulos públicos, commodities, moedas estatais e ações. A frustração com o sistema financeiro corrente derivava em grande parte de uma decepção com a falta de fidúcia exercida pelos grandes intermediários dos mercados de capitais. Os controles de risco existentes nos bancos não foram suficientes para frear os excessos de alavancagem dos *go-go years* do novo milênio, e o interesse pelas taxas envolvidas no financiamento imobiliário (e suas derivações) gerou a maior crise financeira das últimas décadas, colocando em xeque a própria viabilidade do sistema financeiro mundial.

Depois do centenário Lehman Brothers declarar falência, ninguém sabia quem poderia quebrar da noite para o dia e os bancos perderam a confiança de emprestar dinheiro uns para os outros até no *overnight* (empréstimo de um dia com garantia real usado massivamente pelos bancos para fechar seus balanços, equivalente à nossa "compromissada"). Os governos precisaram entrar em cena e usar o suado *Taxpayer Money* para garantir primeiro a liquidez e depois a solvência do sistema como um todo. Foi implementado o maior plano de resgate e injeção de capital em mercados privados já vistos desde a criação dos governos. Doze anos depois (2020) a gente revisitaria esses recordes, mas isso é papo para outra carta.

Ou seja, após quase uma década de riscos e recompensas exorbitantes, era o dinheiro do cidadão que estava sendo diluído para garantir que o resto da economia não afundaria junto com os bancos. Os intermediários do sistema financeiro eram *too big to fail* (grandes demais para quebrar), e ninguém quis correr o risco de uma quebradeira geral, com todo mundo relembrando 1929 como se fosse ontem.

Acontece que os bancos não ocupam o espaço que ocupam hoje por mero acaso. Em um mundo de transações pontuais entre desconhecidos, a figura do intermediário é essencial para garantir que o dinheiro que você envia para comprar um jogo novo para o seu filho é realmente seu. Aquele que recebe o dinheiro confia muito mais no banco do que em você, afinal, ele não te conhece e na maioria dos casos não sabe como lhe cobrar. Acrescente-se a isso um mundo de digitalização crescente, onde o dinheiro é majoritariamente representado por registros em bases de dados, onde nada impede que repetidos “CTRL+C e CTRL+V” permitissem que você comprasse não só o jogo novo, como também a própria empresa que desenvolve o jogo (conhecido como gasto duplo). No final das contas, o que nos impede de perder completamente a confiança no dinheiro é o depósito dessa confiança em um intermediário.

Faz sentido, diante dessa perda de confiança observada na crise de 2007–08, que os insatisfeitos intensificassem a exploração de um arranjo monetário paralelo e interoperável com o sistema legado, que reduzisse a dependência de garantias de bancos e governos. Um dinheiro nativamente digital com validação aberta poderia atenuar essa dor ao deslocar parte da verificação de “quem devo confiar” para regras verificáveis por qualquer participante, reduzindo pontos únicos de falha e a necessidade de intermediários para prevenir gasto duplo.

A possibilidade de gasto duplo tornava qualquer tentativa de dinheiro digital inimaginável, afinal, um arquivo de computador contendo um saldo poderia ser facilmente copiado infinitamente. A necessidade de um intermediário de confiança, como no dinheiro tradicional, criava risco de arbitrariedade, falhas e custos. Garantir uma oferta realmente limitada, que não pudesse ser deliberadamente diluída após uma canetada, criar um mecanismo de consenso eficiente e objetivo, e mesmo assim assegurar a imutabilidade das transações, eram os principais desafios.

O desafio posto era conseguir criar uma moeda digital escassa e cujas transações pudessem ser validadas de forma descentralizada, ou seja, sem a necessidade de um intermediário de confiança que verificasse a unicidade de cada registro monetário e a veracidade dos recursos transacionados. Mas como dispensar o intermediário e permitir transações anônimas entre desconhecidos digitalmente?

A solução para estes problemas foi descrita por Satoshi, no paper Bitcoin: A Peer-to-Peer Electronic Cash System. Mais do que teoria, a arquitetura se sustentou na prática: em janeiro de 2009, Satoshi envia 10 BTC para Hal Finney, um dos primeiros desenvolvedores a acreditar no projeto.

A solução

No modelo tradicional, um banco/clearing mantém um livro-razão central (ledger), carimba a ordem temporal e define o que é uma transação válida e nós confiamos nele. No Bitcoin, esse mesmo livro-razão é distribuído: milhares de computadores (nós) rodam um software aberto e verificam se as regras definidas no protocolo Bitcoin foram atendidas em cada conjunto novo de transações (bloco) e mantêm uma visão comum do estado atual das posições em Bitcoin.

Qualquer pessoa pode baixar um *client* (o mais usado é o Bitcoin Core) e rodar um nó, contribuindo para a segurança ao fiscalizar regras e propagar a criação de novos blocos e as solicitações de novas transações. Em termos de design, isso troca o carimbo de tempo central por um servidor de *timestamp* distribuído: a rede inteira garante a ordem das transações por meio da inclusão em blocos e do consenso entre os nós. Isso evita que a mesma moeda seja reaproveitada (gasto duplo). No arranjo antigo, esse carimbo e a auditoria viriam da instituição financeira e de seus sistemas de reconciliação; aqui, vêm de um protocolo aberto executado por pares.

E como uma nova transação entra no livro? No sistema bancário, você manda uma ordem, o banco confere se você é você mesmo, se o saldo existe mesmo, aplica regras internas e liquida via sua própria infraestrutura. No Bitcoin, você solicita a transação e ela é espalhada pela rede (*gossip*), os nós a recebem, verificam regras iniciais de validade (assinaturas digitais de autenticação das transações, coerência da origem dos fundos, formato da solicitação etc.) e essa transação é adicionada a uma fila de transações pendentes.

No Bitcoin, a escassez vem de uma regra do protocolo: só existirão 21 milhões de unidades, e a emissão de novas moedas vai diminuindo ao longo do tempo, em etapas chamadas de halving.

A validação das transações, por sua vez, acontece por meio de uma loteria econômica chamada Prova de Trabalho (PoW). É aí que entram os mineradores. Eles juntam as transações que ouviram e tentam encontrar aleatoriamente um “bilhete” vencedor. Achar esse bilhete é uma tarefa computacional hercúlea que custa energia e requer muitas tentativas, mas a verificação de validade do bilhete pode ser feita instantaneamente em um passo computacional.

Glossário

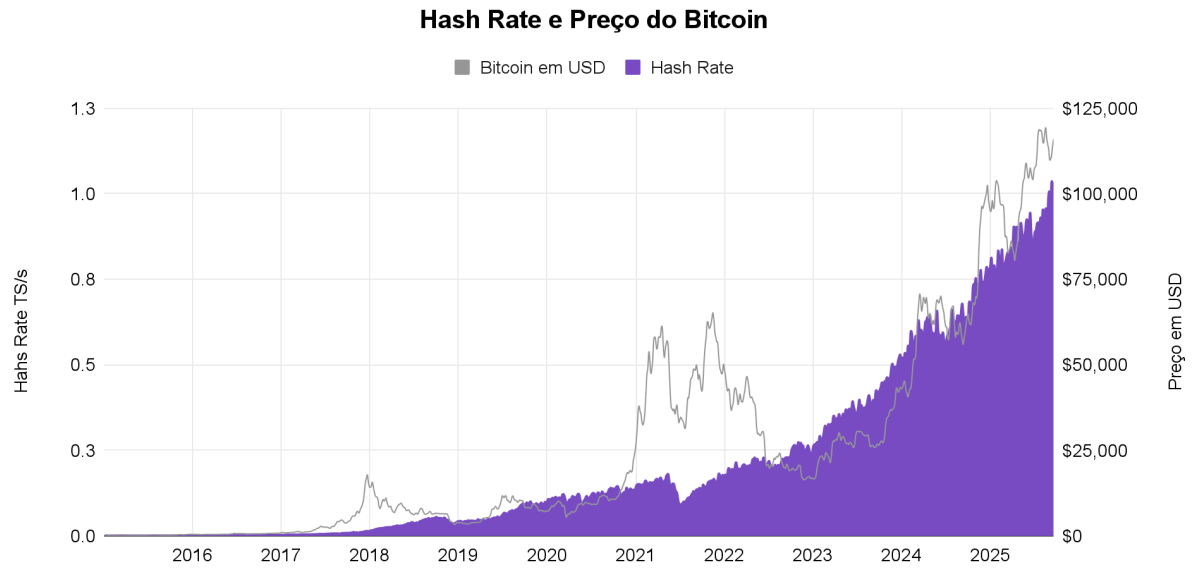
Blockchain: registro público e descentralizado que armazena cronologicamente todos os blocos de transações.
Bloco: conjunto de transações agrupadas e registradas de forma imutável na blockchain.
BTC: sigla para Bitcoin, a primeira e mais conhecida criptomoeda digital.
Duplo gasto: tentativa fraudulenta de gastar a mesma unidade de Bitcoin mais de uma vez.
Gossip: protocolo de disseminação de dados em que os nós compartilham informações com seus pares.
Halving: evento que reduz pela metade a recompensa por bloco minerado, ocorrendo aproximadamente a cada 4 anos.
Hash rate: medida da capacidade total de processamento computacional dedicada à mineração de Bitcoin.
Mineradores: participantes que usam poder de processamento para validar blocos e receber recompensas em Bitcoin.
Nós: computadores que participam da rede Bitcoin validando e retransmitindo transações.
Pares: outros nós conectados que trocam informações diretamente entre si na rede.
PoW: sigla de Proof of Work, mecanismo de consenso baseado em poder computacional para validar transações.
Rodar um nó: operar um software que mantém cópia atualizada da blockchain e valida transações.
Wallet: carteira digital usada para armazenar e gerenciar chaves privadas e transações de Bitcoin.

Os mineradores reúnem as transações até preencher a capacidade do bloco. Esse limite já foi de 1 MB no desenho original, mas hoje a forma de medir mudou e os blocos podem acomodar um pouco mais de dados. Quando o bloco é completado, ele é fechado e encadeado aos blocos de transações anteriores (*blockchain*). E quando um bloco é produzido, todos enxergam as transações incluídas, e cada nó pode realizar uma checagem independente e imediata de que o novo bloco gerado atende às regras do protocolo Bitcoin, inclusive de que não houve gasto duplo. No modelo tradicional, a garantia vem de controles internos e eventualmente de auditorias; aqui, vem de verificação pública, automática e padronizada pelos nós. A confiança é deslocada do intermediário decisor para a comunidade de computadores que formam a rede. Ao invés de uma entidade dizer “ok”, milhares de nós independentes rejeitam qualquer tentativa de fraude e só aceitam o que passa nas regras comuns.

A cada novo bloco criado, além das taxas associadas a cada transação, novos bitcoins são emitidos e entregues ao minerador portador do bilhete premiado (atualmente 3,15 são gerados por cada bloco). Isso aproxima gradualmente a quantidade de tokens disponíveis de sua quantidade final de 21 milhões. Mas, diferentemente do sistema tradicional, isso é feito de forma

previsível e controlada. Inclusive a própria rede ajusta o alvo/dificuldade da loteria conforme a velocidade recente de criação de novos blocos para manter estável o ritmo de emissão de novos bitcoins. No mundo tradicional, esse “ritmo” fica a cabo dos Bancos Centrais atuando em conjunto com interesses dos governos vigentes.

No Bitcoin, “travar a história” significa tornar proibitivamente caro reescrever blocos, ou seja, é preciso refazer a Prova de Trabalho acumulada por toda a rede a partir de certo ponto. Essa segurança é, na prática, função do *hash rate*: quanto maior o poder computacional somado, mais trabalho é empilhado por segundos sobre cada bloco e mais improvável fica qualquer ataque. O gráfico a seguir mostra a evolução desse hash rate.



Vale comentar também o cuidado com o desenho de incentivos do protocolo como um todo. Minerar produz recompensa de bloco e taxas, mas só se o bloco seguir as regras aceitas pelos nós; se um minerador tentar “se pagar mais” ou violar o protocolo, os demais nós rejeitam e aquele esforço vira energia queimada em vão. Usuários/investidores e empresas que aceitam BTC têm poder econômico: se uma maioria tentasse corromper o ativo (ex.: inflacionar oferta), o mercado puniria no preço; uma minoria intolerante sempre pode manter as regras originais rodando seus próprios nós. Em suma: (i) é livre-entrada (qualquer um roda nó/minera), (ii) é caro trair e barato verificar, (iii) a coordenação de consenso é automática (cadeia com mais trabalho) e (iv) os ganhos estão no comportamento honesto.

Inclusão em um portfólio

A natureza única do Bitcoin faz dele um ativo difícil de ser enquadrado nas classes tradicionais. Em janeiro deste ano, a Coinbase, em parceria com a EY, pesquisou 352 gestores institucionais — incluindo hedge funds, private banks, venture capital e family offices — para entender como eles classificam os ativos digitais. O estudo mostrou que não há consenso: parte os considera como Alternatives, outra como Commodities, e 44% criaram uma categoria própria de “Crypto” ou “Digital Assets” em suas alocações.

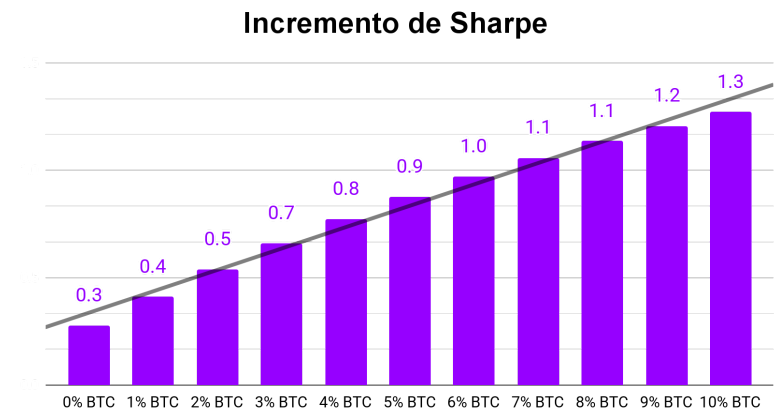
Quando analisamos a correlação do Bitcoin com os principais betas de um asset allocation no Brasil, o fator diversificação fica evidente. Nos últimos 15 anos, a maior correlação é com o S&P 500 (em reais), com apenas 27%.

Um exercício prático para entender o papel dele em um asset allocation é adicionar proporções em um portfólio teórico, contendo 60% IMA-B e 40% S&P 500 em reais. É chover no molhado comparar os retornos quando adicionamos bitcoin na alocação por conta dos retornos expressivos, mas podemos analisar o incremento de Sharpe. Dessa forma, o acréscimo de retorno precisa ser compensado pelo acréscimo de volatilidade - afinal de contas, é um ativo cuja volatilidade frequentemente está acima de 50%.

Correlação

	Bitcoin	*Dólar*	*Ibovespa*	*S&P 500*	*Ouro*	*IMA-B*
Bitcoin	100%	17%	3%	27%	17%	-7%
Dólar	17%	100%	-50%	53%	70%	-49%
Ibovespa	3%	-50%	100%	9%	-35%	55%
S&P 500	27%	53%	9%	100%	36%	-16%
Ouro	17%	70%	-35%	36%	100%	-33%
IMA-B	-7%	-49%	55%	-16%	-33%	100%

Fonte: Bloomberg. Dados entre jan/2015 e set/2025.



Partindo de um portfólio 60-40 e diluindo este portfólio proporcionalmente para adicionar bitcoin, fica claro que a relação risco x retorno é muito bem recompensada. O portfólio base sai de um Índice Sharpe de 0,3 para 0,4 (acréscimo superior a 30%), adicionando apenas 1% em Bitcoin. Os ganhos mais expressivos de Sharpe concentram-se em até 5%. Mais do que isso, o incremento é marginal, e a volatilidade dos portfólios se torna insuportável para a maioria dos investidores.

Falando em volatilidade, esse sempre foi um ponto que prejudicou a imagem do ativo, a ponto de muitos investidores sequer considerarem sua inclusão em portfólios. No entanto, a volatilidade vem se reduzindo de forma consistente. Para se ter uma ideia, caiu de 74% em 2021 para os atuais 44%. A melhora é fruto da recente repercussão, do lançamento de ETFs de bitcoin nos Estados Unidos — incluindo o fundo da BlackRock, que já bateu recordes históricos de captação — de empresas adicionando bitcoin ao caixa, como a MicroStrategy, e do crescente interesse de investidores institucionais.

Desafios da autocustódia

Para montar sua própria carteira e começar a acumular Bitcoin, o primeiro passo é escolher qual *wallet* utilizar. Pode ser uma *hard wallet*, como Ledger ou Trezor, ou uma *hot wallet,* como Metamask ou Electrum. Depois disso, é preciso gerar uma nova carteira. Nesse processo, será criado um seed (12 ou 24 palavras) que dará origem às chaves públicas e à chave privada. É fundamental anotar esse *seed* em papel ou placa metálica e guardá-lo em um local seguro.

Quem tiver acesso à sua chave privada terá controle total da sua *wallet* — e não existe suporte ou central de atendimento a quem recorrer. Se você perder o backup, seja por roubo, incêndio ou simplesmente por ter esquecido onde guardou, não há como recuperar: os fundos são perdidos para sempre. Há ainda a questão da herança, que exige planejamento para garantir que seus filhos ou herdeiros consigam receber de fato as criptomoedas.

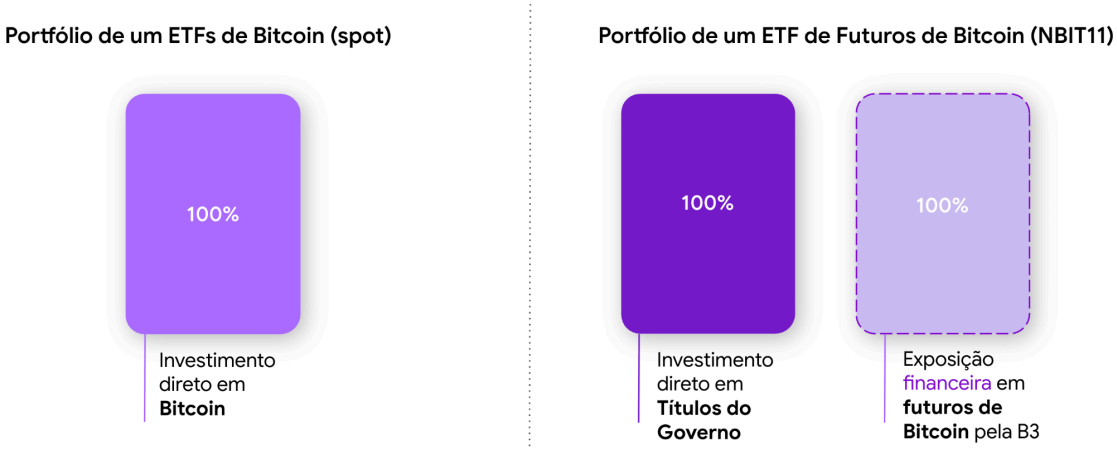
Fonte: https://www.chainalysis.com/
Fonte: https://crystalintelligence.com/investigations/the-10-biggest-crypto-hacks-in-history/

O gráfico anterior ilustra a distribuição dos 21 milhões de BTC: cerca de 1,1 milhão pertencem a Satoshi, aproximadamente 3,7 milhões (18%) estão perdidos, 14,8 milhões estão em circulação e 1,4 milhão (7%) ainda restam a ser minerados. Esses números reforçam os riscos da autocustódia e evidenciam o impacto de *hacks*, que já somam perdas de US$4,2 bilhões.

NBIT11

Para investidores que preferem evitar os riscos e complexidades da autocustódia, existem alternativas mais seguras e práticas no mercado tradicional. Pensando nisso, a Nu Asset lançou o NBIT11, um ETF que dá exposição **sintética** ao Bitcoin via contratos futuros (BIT) da B3. Esses contratos começaram a negociar em 17/abr/2024 e, em um ano, superaram R$2 trilhões em volume financeiro, com picos diários acima de R$10 bilhões em sessões pontuais. O NBIT11 replica o Nasdaq Brazil Bitcoin Futures TR Index (NQBTCBRT) — desenvolvido em parceria com a Nasdaq, que mede o retorno total do contrato mensal mais próximo (símbolo BIT) negociado na B3. O índice considera tanto a exposição ao futuro (ajustes diários) quanto o rendimento do caixa (margem), refletindo a dinâmica de um índice *total return*.

A estrutura separa colateral e exposição: em vez de deter BTC, o fundo aloca 100% do patrimônio em títulos públicos de alta liquidez e, simultaneamente, assume 100% de exposição comprada via futuros de Bitcoin (BIT) na B3. O retorno total combina o ajuste diário do futuro com o rendimento do colateral, oferecendo exposição econômica ao Bitcoin com custódia tradicional..



Como o Nu Seleção está investindo em bitcoin

Nos últimos anos, a decisão de não ter cripto passou a ser uma decisão ativa de risco: a classe entrou no *set* de ativos considerados por alocadores institucionais e, em testes proprietários (jan/2015–set/2025), a inclusão pequena e controlada de Bitcoin elevou a eficiência do portfólio. Em particular, 3–4% de BTC no mix histórico dobrou o Sharpe do portfólio-base e acima disso, o ganho marginal persiste, mas com retornos decrescentes. Esse resultado é consistente com a literatura institucional, que costuma apontar janelas ótimas entre 1% e 5% de alocação.

Do lado da exposição a risco, os impactos são manejáveis quando a posição é contida. Com uma exposição de apenas 2,2% de bitcoin no Nu Seleção Master, o CAGR subiu de 11,7% para 13,7%, com a volatilidade marginalmente subindo de 6,5% para 6,7%. Isso implica em um ganho de Sharpe Ratio de 0,33 para 0,59 e tudo isso com um Drawdown Máximo praticamente estável reforçando o caráter complementar desta classe de ativo nos portfólios.

AVISO LEGAL

Nu Seleção Potencial

Categoria Anbima	**Multimercados Dinâmico**
CNPJ do fundo	**40.156.155/0001-36**
Gestor	**Nu Asset Management LTDA**
Administrador	**Intrag DTVM**
Auditoria	**PriceWatershouseCoopers**
Tributação	**Regressiva de longo prazo**
Taxa de administração	**0,50% a.a.**
Taxa de administração máxima	**0,70% a.a.**
Taxa de performance	**Não possui**
Aplicação inicial	**R$ 100,00**
Investimento adicional mínimo	**R$ 1,00**
Saldo mínimo	**R$ 100,00**
Cota de aplicação	**D+1 d.u**
Cota de resgate	**D+2 d.u**
Disponibilização de recursos	**D+3 d.u**
Data de início	**16/03/2021**
Patrimônio líquido (29/08/2025)	**R$29,981,811.87**
Patrimônio líquido médio - 12 meses	**R$37,163,686.30**
Rentabilidade nos últimos 12 meses	**5.87%**

Nu Nasdaq Brazil Bitcoin Carry Futures

Código de Negociação	**NBIT11**
Gestor	**Nu Asset Management LTDA**
Administrador e Custodiante	**Banco BNP Paribas Brasil S.A**
Provedor do Índice	**Nasdaq**
Formador de Mercado	**BTG Pactual**
Taxa Global (decrescente - vide pág. 2)	**0,50% a.a. (Máxima: 0,60% a.a.)**
Taxa de Performance	**N/A**
Índice de Referência	**NQBTCBRT**
Código ISIN	**BRNBITCTF002**
Público Alvo	**Investidores em Geral**
Data de Ínicio	**19/08/2025**
Liquidação	**D+2 d.u**
Rebalanceamento	**Mensal**
CNPJ	**61.846.717/0001-43**
Patrimônio Líquido (29/08/2025)	**R$4,698,845.86**
Classificação Anbima	**ETF de Renda Variável**
Auditor	**PwC**
Tributação	**Renda Variável**
Distribuição de Rendimentos	**Não há**

Contribuidores

Victor Duran, CFA
Quantitative Researcher Specialist
victor.duran@nubank.com.br

Rafael Rossi
Quantitative Researcher
rafael.rossi@nubank.com.br