Pontifícia Universidade Católica
do Rio de Janeiro

Hugo De Carlo Rocha Filho

Análise de investimento de mineração de *Bitcoin* sob condições de incerteza

Dissertação de Mestrado

Dissertação apresentada como requisito parcial para obtenção do grau de Mestre pelo Programa de Pós-graduação em Administração de Empresas da PUC-Rio.

Orientador: Prof. Leonardo Lima Gomes

Rio de Janeiro

Abril de 2019

Pontifícia Universidade Católica
do Rio de Janeiro

Hugo De Carlo Rocha Filho

Análise de investimento de mineração de *Bitcoin* sob condições de incerteza

Dissertação apresentada como requisito parcial para obtenção do grau de Mestre pelo Programa de Pós-Graduação em Administração de Empresas da PUC-Rio. Aprovada pela Comissão Examinadora abaixo assinada.

Prof. Leonardo Lima Gomes
Orientador
Departamento de Administração – PUC-Rio

Prof. Luiz Eduardo Texeira Brandão
Departamento de Administração - PUC-Rio

Prof. Carlos de Lamare Bastian Pinto
Pesquisador Autônomo

Rio de Janeiro, 15 de abril de 2019

Hugo De Carlo Rocha Filho

Graduado em Tecnologia pela PUC-Rio (2000), MBA em Gestão de Projetos pela FGV(2005) e MBA em Management pela PUC-Rio(2016). Experiência de 19 anos no mercado corporativo, atuando em na área de Tecnologia da Informação em multinacionais e organizações de diversos segmentos: Telecomunicações, Indústria, Militar e Ensino.

Ficha Catalográfica

Rocha Filho, Hugo De Carlo

Análise de investimento de mineração de *bitcoin* sob condições de incerteza / Hugo De Carlo Rocha Filho; orientador: Leonardo Lima Gomes. – 2019.
67 f. : il. color. ; 30 cm

Dissertação (mestrado)–Pontifícia Universidade Católica do Rio de Janeiro, Departamento de Administração, 2019.
Inclui bibliografia

1. Administração – Teses. 2. Mineração de bitcoins. 3. Análise de viabilidade. 4. Métodos estocásticos. I. Gomes, Leonardo Lima. II. Pontifícia Universidade Católica do Rio de Janeiro. Departamento de Administração. III. Título.

CDD: 658

Agradecimentos

À minha mãe, **Léa Ferraz**, que é tudo na minha vida! É meu porto seguro, a pessoa que me dá segurança quando o mundo parece ruir, que me incentiva em todos os meus sonhos e me dá forças para lutar, seguir em frente e superar qualquer obstáculo. Uma mulher de garra que tenho profunda admiração, gratidão e amor. Desde que eu era pequeno, além de valores morais e de generosidade ao próximo, sempre me mostrou a importância do estudo para meu futuro. Nada disso teria sido possível sem você!

À minha esposa **Mônica Muhlbauer**, pelo companheirismo, compreensão e apoio durante todo curso e pelo constante incentivo para eu ingressar na área acadêmica. A minha filha **Fernanda De Carlo** pelo imensurável entendimento dos momentos em que teve de abdicar da minha presença para que eu pudesse completar esta etapa tão importante de minha formação. “A família deve ser a base de tudo e com ela qualquer coisa pode se conquistar e superar”

Ao meu orientador, professor **Leonardo Lima**, pela atenção, paciência, pelas valiosas contribuições que fez neste trabalho e horas em que concedeu seu tempo para debatermos sobre o mercado de criptoativos, contratos inteligentes, mineração e do poder disruptivo da Blockchain. Sem sombra de dúvidas considero uma honra tê-lo como orientador.

Ao amigo **Cid Leonardo**, que me apresentou o mundo das criptomoedas e montou nossa primeira mineradora, utilizando ainda placas gráficas! Infelizmente a infraestrutura que montamos hoje não está mais ativa. Porém, foram grandes planos e ficam as lembranças das excelentes discussões e incontáveis conversas sobre o tema abordado na dissertação

Aos amigos que fiz no MBA Management e no mestrado! Em especial **Cláudia Bozza**, **Vinicius Giglio e Thomas Campos**, pelas horas em que estudamos juntos, pelas grandes apresentações e trabalhos que fizemos durante praticamente todas as matérias e pela mútua admiração, ajuda, incentivo e confiança que tivemos ao longo do curso.

Resumo

Filho, Hugo De Carlo Rocha; Gomes, Leonardo Lima. **Análise de investimento de mineração de Bitcoin sob ambiente de incerteza**. Rio de Janeiro, 2019. 67p. Dissertação de Mestrado - Departamento de Administração, Pontifícia Universidade Católica do Rio de Janeiro.

O presente trabalho se propôs a efetuar uma investigação resumida do mercado de mineração de criptomoedas no Brasil e analisar a viabilidade econômica da implantação de uma fazenda de mineração de Bitcoins em território brasileiro. O estudo foi realizado em três etapas, onde foram abordadas análises determinísticas baseadas em possíveis cenários, observação da sensibilidade do investimento em relação as principais variáveis do problema e por último a utilização de métodos estocásticos visando estimar o risco do investimento, em razão do ambiente de incerteza. Os resultados demonstram que este é um investimento de altíssimo risco e que não existe viabilidade econômica em minerar Bitcoin no Brasil, com cotação do abaixo de US$ 10.065. O estudo aponta o custo da energia elétrica como o mais expressivo, seguido do investimento nos equipamentos de mineração e sugere que a operação seja estabelecida em países com menor custo de eletricidade, clima mais baixo e menores taxas de importação e de imposto de renda.

Palavras-chave

Mineração de Bitcoins; Análise de viabilidade; Métodos estocásticos.

Abstract

Filho, Hugo De Carlo Rocha; Gomes, Leonardo Lima (Advisor). **Analysis of investimento in Bitcoin mining under uncertain**. Rio de Janeiro, 2019. 67p. MSc. Dissertation - Departamento de Administração, Pontifícia Universidade Católica do Rio de Janeiro.

This work carries out a brief investigation of cryptocurrencies mining market in Brazil and to analyze the economic viability of the investment in a Bitcoin mining farm in Brazil. The study was carried out in three stages, where deterministic analyzes were based on possible scenarios, observation of the sensitivity of the investment relative to the main variables of the problem and finally the use of stochastic methods to estimate the investment risk under uncertainty. The study points to the cost of electricity as the most significant, followed by investment in mining equipment and suggests that the operation be established in countries with lower electricity costs, lower climate and lower import and income tax rates.

Keywords

Bitcoin Mining; Feasibility Analysis; Stochastic Methods.

Sumário

Lista de figuras

Lista de tabelas

1
Introdução

O Bitcoin é uma moeda digital e primeiro sistema de pagamento online descentralizado do mundo que resolveu o problema do gasto duplo (NAKAMOTO, 2008). O projeto surgiu como antítese ao sistema financeiro durante a crise econômica do ano de 2008 e ambicionava a ruptura do sistema bancário, descentralização do sistema financeiro, supressão do controle monetário dos governos e redução das altas taxas cobradas pelas intermediações.

Este é um sistema baseado em software que implementa um protocolo de confiança doravante denominado Blockchain. O surgimento dessa tecnologia permitiu a criação de transações diretas entre partes interessadas sem a necessidade de passar por uma instituição fiduciária, para garantir a confiança das operações. Isso só foi possível após a publicação do artigo Peer-to-Peer Electronic Cash System e desenvolvimento do sistema Blockchain, por (NAKAMOTO, 2008) que apresentou a primeira solução no mundo para impedir o gasto duplo de criptomoedas. Este feito foi alcançado através da combinação de tecnologias existentes tais como a rede *peer-to-peer*, criptografia e assinatura digital, para criar uma estrutura de dados pública que funciona como um livro-razão transparente, compartilhado, imutável e persistido, entre os nós da rede, de forma cronológica.

Os mineradores, são os principais agentes desse ecossistema e tem como objetivo alcançar, por consenso, a confiança das transações e garantir a manutenção do livro-razão. O consenso é obtido através da solução de problemas matemáticos que exigem o emprego de poder computacional para descobrir, por força bruta, a assinatura do bloco a ser inserido, que também contém o identificador do bloco anterior. O sistema recompensa com Bitcoins o primeiro minerador que conseguir descobrir essa chave, que permite a gravação do bloco na rede, após validação dos nós que a compõem. Esse processo continua indefinidamente pelos próximos blocos remunerando os constituintes da infraestrutura dessa cadeia que lograram sucesso na descoberta do desafio criptográfico. O sistema é seguro, pois nós honestos controlam coletivamente

mais poder de processamento (CPU) do que qualquer grupo de nós atacantes e quanto maior for a cadeia, mais difícil será fraudá-la (NAKAMOTO, 2008).

A criptomoeda foi inicialmente utilizada por entusiastas de criptografia, tecnologia e desenvolvimento. Entretanto, um dos primeiros usos comerciais foi no mercado ilegal, uma vez que era possível efetuar transações diretas entre as partes interessadas, de forma pseudoanônima. Após ações de combate ao mercado ilícito e reposicionamento do uso da criptomoeda, por volta do ano de 2013, o Bitcoin passou a ser conhecido em outros mercados e com isso, teve uma surpreendente valorização de 5.585% no ano de 2013, quando passou de US$13, a valer US$739,00 no final do referido ano. Desde então, a criptomoeda não parou de ganhar destaque e notoriedade, até se tornar a moeda virtual mais popular do mundo. E com isso houve um número cada vez maior de transações e de novos mineradores investindo em infraestrutura e poder computacional para suportar essa rede de pagamento. Apesar da alta volatilidade o investimento continuava a apresentar altas acima das praticadas em mercado e atrair cada vez mais o interesse pelo assunto. Em 2018 o mundo viu Bitcoin desabar e perder mais de 70% do seu valor, após uma alta de 1833% no ano anterior, quando a moeda registrou seu pico histórico, próximo a US$20.000(vinte mil dólares). Essa enorme desvalorização abalou o mercado de mineração, forçando diversos mineradores a encerraram suas atividades, que acarretou na primeira redução drástica do poder de processamento da rede, que precisou reduzir o nível de dificuldade em 32%, para manter o interesse dos mineradores e o processamento dos blocos a cada dez minutos. Neste episódio, acometida por esta crise, uma das maiores empresas de mineração de criptomoedas, a Bitmain, demitiu 50% dos funcionários e postergou planos para expansão de suas atividades.

Isto posto, este trabalho pretende analisar a viabilidade econômica de investir na montagem de uma fazenda de mineração de Bitcoin e responder a seguinte pergunta de pesquisa: Apesar de inúmeros riscos, será que é lucrativo investir em mineração de Bitcoins no Brasil? Para se atingir o objetivo final proposto esse estudo prevê, como objetivos intermediários a serem alcançados a análise das principais variáveis envolvidas no problema e o desenvolvimento de um modelo de fluxo de caixa para cálculo de viabilidade. O escopo da pesquisa volta-se mais especificamente na avaliação de um projeto de implementação de mineração de Bitcoins no Brasil, com capacidade até 100 máquinas. Embora relevante, não se pretende tratar da mineração em larga escala e/ou datacenters, e nem em outros países, já que tais perspectivas

exigem conhecimentos específicos fora do âmbito financeiro, que é o foco desta pesquisa.

2
Referencial teórico

Nesta seção são apresentados aspectos teóricos e estudos relacionados ao tema de investigação. Entretanto, como tema é ainda pouco discutido e com pequena literatura acadêmica disponível, esta seção busca, alternativamente, discorrer sobre os artigos mais relevantes, que contribuem ou se relacionam, mesmo de forma indireta, com o objetivo deste trabalho.

2.1.
Bitcoin

O Bitcoin foi apresentado ao mundo em outubro de 2008, quando foi publicado, em uma lista de discussão online de criptografia, um estudo que propunha resolver o problema do gasto duplo das criptomoedas e ser o primeiro sistema de pagamento descentralizado do mundo, que permitiria que pagamentos on-line fossem enviados diretamente, de uma entidade para outra, sem a necessidade de passar por uma instituição financeira para validação da transação (NAKAMOTO, 2008). De acordo com informações obtidas no site http://historyofbitcoin.org , o software foi registrado em um site de colaboração, focado no desenvolvimento de código aberto, e no dia 3 de janeiro de 2009, ocorreu sua primeira transação, com o registro do seu bloco gênesis. A moeda era conhecida apenas em fóruns específicos de discussão de criptografia e desenvolvimento de código aberto. No dia 22 de maio de 2010, foi efetuada a primeira transação no mundo, em que uma mercadoria tenha sido trocada por criptomoedas. Neste fato histórico, para o Bitcoin, foram gastos 10.000 BTC para comprar uma fatia de pizza. Em novembro deste mesmo ano o Market CAP já excedia mais de 1 milhão de dólares. Porém em razão da sua estrutura o Bitcoin era primordialmente utilizado apenas pelos mercados alternativos ou ilícitos. Em abril de 2011 a revista TIME publicou o primeiro artigo sobre a moeda, questionando se o dinheiro online poderia desafiar governos e bancos. No final do ano de 2012 foi criada a fundação Bitcoin, que tinha a missão de restaurar a reputação da criptomoeda, além de promover seu desenvolvimento e ampla aceitação. Desde então, o Bitcoin não parou de ganhar destaque e notoriedade, até se tornar a moeda virtual mais popular do mundo, sendo comercializada em

diversos países e com sua aceitação ampliada em diversos mercados. Após forte alta que o Bitcoin obteve no ano de 2013, a criptomoeda passou por uma forte correção nos dois anos seguintes. Em 2016 a moeda passou a registar novo canal de alta, quebrando a resistência do último pico e voltou a registrar ganhos voluptuosos e consecutivos durante todo ano de 2017. O novo pico histórico, cotado em aproximadamente US$20.000 em dezembro de 2017, foi seguido de uma forte correção no ano seguinte que registou uma queda de 70% do valor de mercado.

Existem apenas três formas de obter Bitcoins: através de compra via *exchange*, troca direta com outro usuário, ou então pela atividade de mineração. Para um usuário transacionar Bitcoins, este deve possuir uma carteira virtual, que se assemelha a uma conta corrente, onde é possível calcular o saldo disponível, buscando informações diretamente na Blockchain. Entretanto a carteira não está vinculada ao usuário, como ocorre em um sistema bancário tradicional. Por conseguinte, a administração é efetuada diretamente pelo detentor das credenciais de acesso, que no caso da Blockchain são as chaves públicas e privadas criadas durante a geração da carteira.

Conforme descrito no site Bitcoin.org, a transferência de Bitcoin funciona com base no sistema de criptografia por chave assimétrica, ou seja, para autorizar a saída de criptomoedas de uma carteira, o usuário precisa assinar a transação com sua chave privada, que atua como uma espécie de senha de autorização, que permite os saques desta conta. Para receber Bitcoins é necessário apenas passar o número da carteira, que é criada com base na chave pública. Para registrar na Blockchain a transferência de moedas, a chave privada armazenada na carteira do usuário deve corresponder ao endereço público ao qual a criptomoeda é atribuída.

Conforme dados obtidos no código fonte do Bitcoin, disponível em https://github.com/bitcoin/bitcoin e no *nanodegree* em Blockchain, disponível em udacity.com é descrito processo de criação da carteira que dá-se através de da utilização de diversos algoritmos criptográficos. Em primeiro lugar é criada a chave privada, que pode ser originada de forma determinística, através da inserção de um número base em sua geração, ou produzida de forma completamente aleatória. Esta chave é submetida ao algoritmo Eliptic Curve Digital Signature Algorithm ECDSA, para gerar a chave pública, que por sua vez é utilizada como entrada para o algoritmo SHA-256 para geração do hash criptográfico da chave pública. Este hash é então submetido ao algoritmo RIPEMD160, para produzir um número de 160 bits, que representa a chave

pública do hash. Estes algoritmos são de uma única via, o que significa dizer que é possível conhecer a chave pública através da chave privada, mas que o inverso não é possível. Finalmente a chave pública do hash é submetida ao algoritmo BASE58CHECK, para gerar um número menor e tornar mais clara a leitura do número da carteira, que pode ser compartilhada com os demais usuários da rede, sem temer que as chaves pública ou privada sejam descobertas.

A transferência de Bitcoins ocorre através da transação entre o endereço da carteira de origem e a de destino. A validação dá-se através da assinatura, que é a prova de posse para cada transação ocorrida na Blockchain, uma vez que é assinada usando a chave privada da carteira. A transação por sua vez é compartilhada com os nós da rede. Para descrever todo ciclo de vida e exemplificar o processo, imagine um usuário usr1 que queira enviar um Bitcoin para um usuário usr2. Primeiro usr1 pega o número da carteira de usr2 e cria uma nova transação, informando a transferência de um Bitcoin de sua carteira, para usr2. Nesta transação também será debitado de usr1 a taxa de transação. Uma vez que usr1 possua o saldo disponível, sua carteira inicia a transferência, assinando a transação com sua chave privada. A transação então é distribuída aos nós da rede e fica em uma área de memória cache, conhecida como memory pool, aguardando que os mineradores processem a transação. Os mineradores validam a transferência e por sua vez, agrupam a transação no bloco atual. Assim que for descoberta a prova de trabalho, o bloco é assinado com o valor de hash e então é adicionado à Blockchain. Assim que o bloco ganha confirmações de outros mineradores, essa transação é aceita como válida na rede. Uma vez que a transação seja aceita, o usr2 finalmente recebe o Bitcoin do usr1.

Regra monetária

Tendo em vista que a filosofia por trás do projeto era criar uma rede de pagamento com controle compartilhado e princípios antagônicos ao atual sistema financeiro, foram projetados mecanismos para dar previsibilidade e evitar a inflação da moeda. Foi estabelecido em 21 milhões a quantidade máxima de Bitcoins criados, para caracterizar o efeito de escassez, assim como ouro e outros metais preciosos. Essa medida equipara o Bitcoin a um ativo e assegura que não haverá hiperinflação com a emissão de novas moedas no mercado. O sistema também foi projetado para criar uma emissão progressiva, com o intuito de evitar uma saturação de criptomoedas nos primeiros anos. A

dificuldade de obtenção, foi concebida para se assemelhar ao ouro, onde cada vez fica mais difícil e mais caro minerar as últimas “pedras”. Desta forma, o algoritmo foi desenvolvido para emitir uma quantidade específica de Bitcoins em circulação a cada bloco minerado, que o corre em média a cada 10 minutos. Esta quantidade, paga como recompensa aos mineradores, sofre uma redução pautada em progressão geométrica de razão de 0,5 que é ajustada a cada 210.000 blocos. O que significa dizer que o valor de recompensa é reduzido pela metade em média a cada quatro anos. Esse efeito é conhecido como “*reward halving”.* Quando foi lançada a rede, em março de 2009, a recompensa paga aos mineradores era de 50 btc. No ano de 2012 ocorreu a primeira redução, quando passou a ser pago 25 btc por bloco minerado e posteriormente 12,5 a partir do ano de 2016. Estima-se que a próxima ocorrerá em maio de 2020, quando a recompensa será reduzida para 6,25 btc. Esse processo se repetirá até a emissão da última moeda, previsto para o ano de 2140.

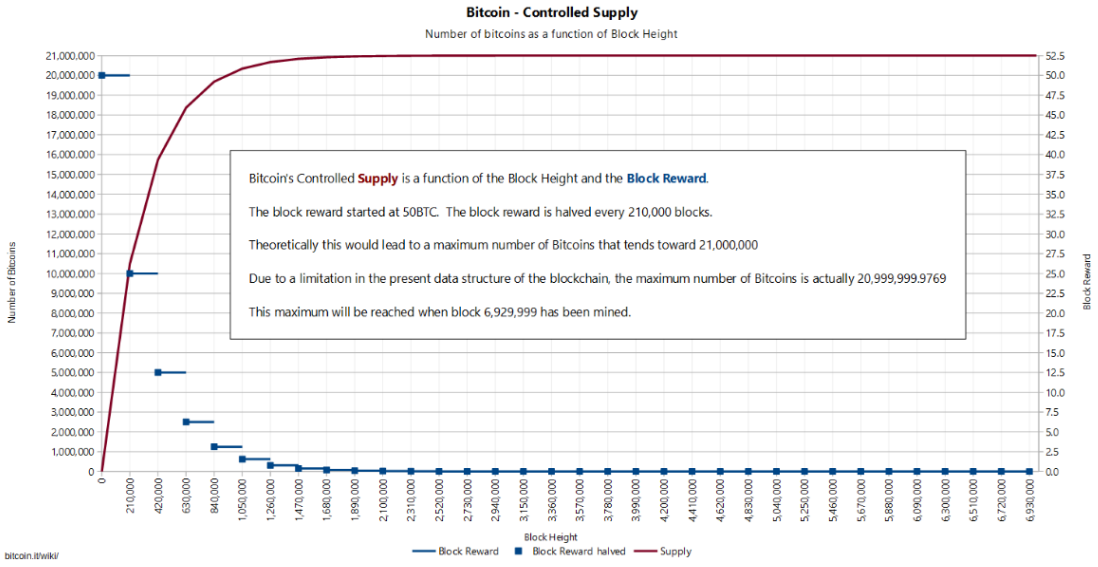


Figura 1: Fornecimento controlado de Bitcoins
Fonte: https://en.bitcoin.it/wiki/Controlled_supply

2.2. Blockchain

Blockchain é um software que surgiu como base para funcionamento do Bitcoin e teve como objetivo principal resolver o controle do gasto duplo e garantir a autenticidade da transação entre duas partes, sem a necessidade de uma entidade intermediadora figurando com alicerce de confiança. Este é um programa de código aberto e colaborativo, o qual sua concepção deu-se através

de estudos oriundos das áreas de engenharia de sistemas, criptografia e estatística. Foram empregados diversos conceitos e tecnologias existentes na criação deste sistema, que implementa um livro-razão descentralizado e compartilhado em uma rede ponto-a-ponto.

Os nós interconectados que a compõem, doravante denominados mineradores, são responsáveis por processar algoritmos de prova de trabalho, que exigem hardwares específicos, poderosos e capazes de trabalhar ininterruptamente para garantir a confiança das transações e mantê-las armazenadas com alta disponibilidade, de forma íntegra, confidencial e imutável.

A rede coloca registros de tempo nas transações que ele insere em uma cadeia contínua de testes de trabalho com base no cálculo de hashes, formando um registro que não pode ser alterado sem recriar o teste de trabalho completo (NAKAMOTO, 2008). Uma vez que a transação é validada ela é copiada para todos nós , que contém lista de transferências legitimadas por consenso pela rede, porém ainda não persistidas no livro-razão. Os mineradores processam um algoritmo de força bruta, que demanda um dispendioso uso de processamento computacional para resolver um problema criptográfico, para um determinado nível de dificuldade estabelecido dinamicamente pelo sistema. Uma vez resolvido o desafio, as transações são inseridas e gravadas sem possibilidade de reversão.

Devido as características de uma rede distribuída é possível que todos os mineradores possuam uma cópia local atualizada do livro-razão e tenham os mesmos direitos e privilégios. O que acarreta com que não exista um dono central da informação e que seja possível chegar a um consenso se a transação é válida, verificando na base de dados se o dinheiro virtual não foi gasto em duplicidade. Isso permite também que mineradores possam entrar ou sair sem causar nenhum impacto ao funcionamento do sistema. Sempre que novo minerador entra na rede, é efetuado um download da cópia completa de todas as transações realizadas na rede desde o bloco Genesis, como é chamado o primeiro bloco da rede, até a mais atual.

A escrituração desta base de dados é realizada através do registro cronológico das transações validadas em determinado período, que são agrupadas em containers lógicos, cognominados blocos. No protocolo Bitcoin, a rede gera, em média a cada dez minutos, um novo bloco, que é encadeado ao bloco anterior. Esse processo continua indefinidamente, formando uma corrente contínua de blocos, o que deu origem ao nome Blockchain. Esse sistema possui uma robusta estrutura de dados alicerçada em complexos e poderosos

algoritmos criptográficos para garantir a imutabilidade do livro-razão. Além disso se beneficia do poder de crescimento, uma vez que quanto maior a rede, menor é a probabilidade de um ataque bem sucedido.

Estrutura do sistema

Sua organização consiste em uma estrutura encadeada de blocos criptografados que cresce a medida que novos dados são adicionados. O primeiro bloco dessa estrutura é conhecido como bloco Gênesis, que possui um ponteiro para o próximo bloco e assim por diante, sendo possível chegar até o mais recente. Um bloco funciona como container lógico. Sua estrutura é composta por corpo, que possui a lista de transações e cabeçalho, que contém informações de controle para funcionamento do sistema. Visando entre outras funções, garantir a manutenção e coesão da cadeia de dados, além de certificar que nenhuma informação tenha sido adulterada.

Um dos componentes fundamentais deste processo é a função de *hash* criptográfica, que é utilizada para criar uma identidade única para um conjunto de dados. O objetivo desta função é processar os informações de entrada, independentemente do tamanho, e transforma-la em uma saída de tamanho fixo e único. Uma função hash recebe uma entrada e cria uma saída aparentemente aleatória, no entanto, a saída produz um mesmo resultado toda vez que você executa a função em uma determinada entrada e um retorno completamente diferente, caso algum bit seja modificado. Não é possível chegar ao dado de origem pelo hash resultante. Porém é simples comparar se os dados são iguais apenas pela verificação do número hash, que produzirá o mesmo resultado. A função hash utilizada pelo Bitcoin é a SHA256, que retorna um número hexadecimal de tamanho de 256 bits.

Visando gerar maior complexidade e criar uma rede praticamente inviolável, Satoshi Nakamoto desenvolveu um protocolo elaborado para garantir que qualquer informação adulterada seja facilmente detectada e invalide o bloco na qual está contida. Por sua vez, isso tornará nula a cadeia de dados existente após a violação. Cada bloco possui um identificador único que é criado a partir do hash de seu cabeçalho e serve também como prova de validade de toda informação contida nele, incluindo as transações. A fraude só é possível, caso seja recriada toda cadeia desde o bloco adulterado. Porém isso exigirá um processamento descomunal, que terá que superar metade do poder computacional existente em toda rede. Essa possibilidade de violação é conhecida como ataque de 51%. Entretanto, tendo em vista o tamanho atual da

cadeia de blocos e a quantidade de mineradores, que vem crescendo a cada ano, fica cada vez mais difícil falsificar os dados armazenados. Objetivando desestimular esse tipo de ataque, foi adicionado ao protocolo uma taxa de remuneração para os mineradores que mantem o funcionamento da rede. Isso desincentiva o ataque de nós maliciosos, pois, é mais vantajoso cooperar e ser recompensando pela rede do que tentar ataca-la.

Toda transação contida no bloco é registrada na forma de um hash criptográfico, que permite que a informação seja verificada, mesmo sem conhecer seu conteúdo. Esta característica permite que as transações permaneçam anônimas na rede, porém a plataforma é pseudoanônima, pois as identidades estão associadas as suas chaves públicas. Os hashes criptográficos das transações são organizados em uma estrutura de dados conhecida como árvore Merkle, que agrupa as dados em pares, gerando um novo hash para cada junção. Esses números resultantes voltam a ser agrupados em pares sucessivamente até gerar um único hash final, derivado do produto do agrupamento em pares de toda as transações. Este resultado obtido, conhecido como raiz Merkle, é inserido no cabeçalho do bloco para garantir que qualquer modificação nas transações invalide o bloco corrente. Para criar uma dependência forte entre os blocos e gerar uma integridade de toda da estrutura, visando dificultar um ataque na rede, é inserido no cabeçalho do bloco atual o numero de hash do cabeçalho do bloco anterior e o número único (*nonce*) descoberto pelo minerador em sua prova de trabalho, durante a criação do bloco. Isso significa dizer que caso algum bloco seja alterado a corrente é automaticamente invalidada e o atacante terá que efetuar um processamento computacional descomunal para recriar uma nova estrutura de dados válida.

Consenso e prova de trabalho

Tendo em vista que não existe um órgão central que controle a rede, é preciso estabelecer um o mecanismo de votação para ajudar a tomada de decisão a respeito das informações na Blockchain. O Bitcoin utiliza o algoritmo de prova de trabalho para estabelecer o consenso de sua rede. O teste de trabalho envolve a exploração de um valor, de tal forma que, ao calcular um hash, como SHA-256, ele começa com um certo número de bits com valor zero. O trabalho médio necessário será exponencial para o número de bits necessários com valor zero, mas isso pode ser verificado pela execução de um único hash (NAKAMOTO, 2008). A ideia básica por trás deste algoritmo é criar um nível de dificuldade específico, que seja extremamente custoso produzir uma

informação, de tal forma que o tempo e os recursos gastos constituem por si só uma prova para acreditação no resultado do trabalho produzido. Porém não deve ser um tempo extremamente alto, de tal forma que degrade a performance do sistema. Uma vez descoberto o resultado, deve ser possível que os demais nós da rede facilmente validem se a informação está correta e entrem em um consenso, contabilizando um voto por CPU. Esta prova de trabalho exige um alto consumo de energia elétrica para que os mineradores empreguem um poder computacional descomunal na resolução de um desafio matemático complexo, que os habilitem a registrar informações na Blockchain.

O algoritmo implementado no projeto Bitcoin foi projetado para que os mineradores descubram um número único, intitulado NONCE, que é a chave do desafio matemático. Este juntamente com os dados do cabeçalho do bloco atual resultará em um hash criptográfico que inicia com determinado número de zeros exigidos, como prova de dificuldade, pelo sistema. A quantidade de zeros solicitados é variável e diretamente relacionada com o nível de dificuldade estabelecido pela rede para minerar o bloco atual. Isso porque, quanto maior a quantidade de zeros no inicio do hash, mais específico será o número e portanto menos provável que se encontre o NONCE que satisfaça a solução. O que significa dizer que maior será o tempo gasto de processamento para encontra-lo. A probabilidade de encontrar um bloco com o valor de hash zero inicial de 4 bytes é 1 / (2 ^ 32), o que significa que os números médios de "tentativa e erro" são exatamente 2 ^ 32. Uma vez gasto o esforço da CPU para satisfazer a prova de trabalho, o bloco não pode ser alterado sem refazer todo o trabalho. Como blocos posteriores são encadeados depois, o trabalho para alterar um bloco incluiria refazer todos os blocos após ele (NAKAMOTO, 2008).

2.3. Mineração

Os mineradores são similares às infraestruturas de servidores de sistemas comerciais, onde a principal função é prover a infraestrutura segura e necessária para execução dos sistemas da camada de negócio. Mineração é o termo dado as ações executadas pelos nós da rede para criar o consenso distribuído, confirmar a veracidade das transações e manter o livro razão compartilhado. Conforme descrito no artigo A Peer-to-Peer Electronic Cash System (NAKAMOTO, 2008), cada máquina da rede Blockchain é responsável por receber as transações, coleta-las em um bloco e encontrar um número, que representa um desafio criptográfico, que é a prova de trabalho para o conteúdo

do bloco em questão. Assim que uma máquina descobre o valor correspondente ao desafio, ela transmite o bloco para todos os nós da rede, que validam o conteúdo e aceitam o bloco, se todas as transações nele forem válidas e ainda não tiverem sido gastas. Os demais nós expressam a aceitação do bloco trabalhando na criação do próximo bloco da cadeia, usando o hash do bloco aceito como o hash anterior. Existe a possibilidade que mais de um nó encontre simultaneamente o NONCE (número único exigido na prova de trabalho). Neste caso será remunerado o nó que produziu o bloco que pertence a maior cadeia de blocos. Os nós sempre consideram a cadeia mais longa a correta e continuarão trabalhando para estendê-la.

Esse processo para gerar novas criptomoedas é análogo a mineração de ouro, por demandar o emprego considerável de recursos para descoberta de algo valioso, que é escasso e cada vez mais difícil de encontrar ao passar do tempo. Desta forma, a decisão de minerar bitcoins se resume a lucratividade. Um agente racional não realizaria a produção de criptomoedas se incorresse em uma perda real ao fazê-lo (HAYES, 2015). Os mineradores, estão em uma disputa, na qual utilizam algoritmos de força bruta, pautados em tentativa e erro, para descobrir o NONCE.

2.3.1. A importância do nível de dificuldade e do Network *hashrate*

A dificuldade é uma medida de como é difícil encontrar um hash abaixo de um determinado alvo. A variação do nível de dificuldade ocorre para manter o tempo médio de criação do bloco próximo a dez minutos (NAKAMOTO, 2008). Esse número é ajustado a cada 2016 blocos, o que representa duas semanas de registros na Blockchain, para o tempo alvo de criação. Os desenvolvedores do sistema Bitcoin consideraram dez minutos o tempo equilibrado entre segurança e velocidade da rede, uma vez que, um tempo alto tornaria a rede muito lenta e um número muito curto não serviria como uma boa prova de trabalho, pois, não seria tão oneroso produzir uma informação. A dificuldade pode aumentar ou diminuir dependendo da quantidade do poder computacional empregado na rede O ajuste de dificuldade atua como um mecanismo de estabilização, aumentando o custo de produção. A medida que mais potência de mineração agregada é colocada em operação, a dificuldade de mineração aumenta. (HAYES, 2015).

O Bitcoin começou com nível de dificuldade 1 no início de seu funcionamento e permaneceu inalterado durante quase todo ano. Em 31 de dezembro de 2009 foi registrado o primeiro aumento, passando para 1,1829. Enquanto o nível de dificuldade ainda estava baixo, era possível utilizar CPUs multi-core para minerar o bloco. No dia 22 de maio de 2010, quando efetuada a primeira transação no mundo, na qual 10.000 BTC foram trocados por uma pizza, a dificuldade já tinha crescido 901% e estava em 11,8462, mas ainda era possível minerar Bitcoins através de computadores pessoais (CPU). Desde então a rede não parou de crescer, assim como o poder computacional empregado em mineração melhorou muito, e foram criadas máquinas e processadores cada vez mais específicos para resolver o problema. Em 28 de março de 2013, quando o Market cap já havia ultrapassado um bilhão de dólares, a dificuldade estava em 6.695.826,2826. Nove anos após a criação do bloco Genesis o nível de dificuldade subiu para trilhões, de forma que o tempo gasto para minerar um bloco continue mantido em 10 minutos independentemente do tamanho da rede e poder computacional empregado. Em média a rede recalcula esse número a cada duas semanas. Isso ocorre quando o bloco 2016 é gerado. Neste momento o algoritmo verifica quanto tempo levou para produzir esses blocos e divide pelo número obtido o valor alvo, que representa o tempo objetivado pela rede para gerar os 2016 blocos. O quociente desta divisão é multiplicado pelo antigo valor estabelecido, para obter a nova dificuldade. Uma vez ajustado o nível de dificuldade o contador de blocos é zerado e o processo volta a se repetir. Para evitar mudanças abruptas, o algoritmo estipula em 4 o valor máximo de ajuste para qualquer número acima e 0,25 para valores abaixo deste.

2.3.2. Evolução do ecossistema de mineração

O projeto Bitcoin foi concebido para remunerar em criptomoeda as pessoas que empregam seus recursos, infraestrutura, equipamentos, energia elétrica e tempo para garantir a existência e continuidade da rede. No inicio os mineradores usavam seus computadores pessoais, laptops e de suas casas eram capazes de minerar 50BTC a cada dez minutos. É importante considerar o contexto histórico, uma vez que nos seus primeiros anos de existência, o Bitcoin era conhecido apenas em fóruns específicos de discussão de criptografia e desenvolvimento de software. Os usuários da criptomoeda eram basicamente entusiastas de tecnologia e/ou de nichos bem específicos. Por conseguinte o

poder computacional empregado para funcionamento da rede era ínfimo perto do que é utilizado atualmente. Consequentemente o baixo nível de dificuldade da época, permitia a mineração a partir de CPUs. Com a popularização e valorização da criptomoeda, foram introduzidas as placas gráficas (GPU) no processo de mineração, em virtude da velocidade de processamento superior as CPUs. Nesta fase os mineradores individuais montavam estruturas improvisadas para ligar diversas GPUs em placas mães, bem como surgiam as primeiras fazendas de mineração, que são instalações com grande concentração de computadores realizando o processo de mineração. Neste âmbito, em virtude do aquecimento das placas de GPUs e da aglutinação de máquinas, surgiu uma nova variável no contexto da mineração, presente até hoje, que é a necessidade criar sistemas de refrigeração que mantêm todos os computadores operando em uma condição térmica apropriada. Uma terceira fase surgiu com a utilização das placas FPGA, tornando o processo de mineração ainda mais efetivo, em função da velocidade de processamento que acarretou maior poder de processamento da rede e consequentemente aumento do nível de dificuldade, necessário para manter a geração do bloco a cada dez minutos. Essa nova geração inviabilizou o uso de CPUs e criou um desequilíbrio nas estruturas antigas de mineração, visto que a chance de encontrar um bloco com FPGA era muito maior que com as placas gráficas. No final de 2010 surgem os primeiros pools de mineração, que são grupos de mineradores, que unem seu poder de processamento e compartilham os lucros entre os membros. Quanto mais potente for o esforço de mineração (quanto maior o hashate), maior a probabilidade de sucesso de mineração de bitcoins durante um determinado intervalo (HAYES, 2015). A partir do ano de 2013 o processo de mineração atinge outro patamar, com a entrada de máquinas ASICs, desenvolvidas especificamente para o processamento de Bitcoins, com poder computacional excepcionalmente acima das máquinas precedentes e mais eficiente, por requerer menos consumo de energia que as formas anteriores de mineração. A eficiência energética do hardware de mineração já aumentou muito desde os dias de mineração de CPU ou GPU. Um estudo de pesquisa descobriu que a eficiência média da mineração no período 2010-2013 foi de 500 Watts por GH / s (GARCIA *et al*., 2013).

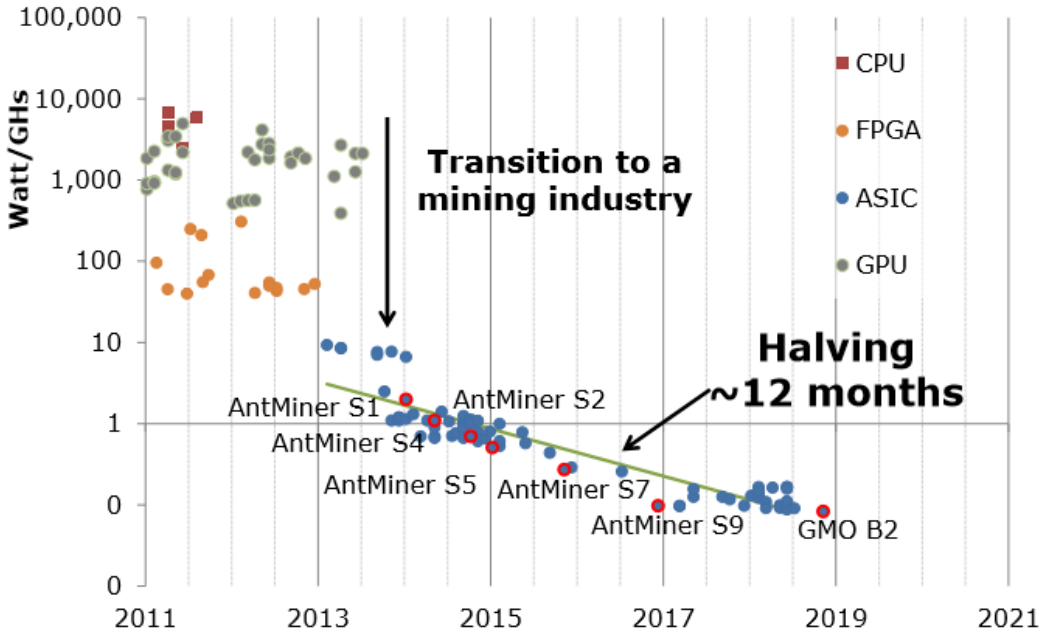


Figura 2: Evolução dos equipamentos de mineração
Fonte:https://www.researchgate.net/publication/328091947_The_Electricity_Intensity_of_Bitcoin_Mining

Ao longo dos anos o ecossistema de mineração evoluiu, foram consolidados mercados de compra e venda de equipamentos, máquinas criadas especificamente para mineração de Bitcoins, surgimento de profissionais voltados à manutenção dos hardwares, projetistas de chips para mineração e a eclosão de estruturas cada vez mais profissionais e sofisticadas, criadas para ganhar em escala e eficiência operacional. Atualmente a mineração está se consubstanciando em grandes pools de mineração, sendo realizada, em grande parte, em datacenters especializados. Estes empregam os equipamentos mais modernos, visando otimizar eficiência energética e poder de processamento em níveis sem precedentes. Além disso, as mineradoras estão se concentrando em regiões com temperaturas mais baixas para diminuir os custos com refrigeração, locais com menor custo de eletricidade, além de menores custos operacionais, regulação e impostos sobre o mercado de criptomoedas.

2.3.3. Dados da mineração na Blockchain

A figura 3 apresenta um gráfico com a participação de mercado dos principais pools de mineração de Bitcoin do Mundo. Nota-se que apesar de uma grande parte dos blocos serem de origem desconhecida, existe um domínio da China, que possui os pools com maiores transações registradas na Blockchain: BTC.com, AntPool, F2Pool, Slush, ViaBTC, DPOOL.

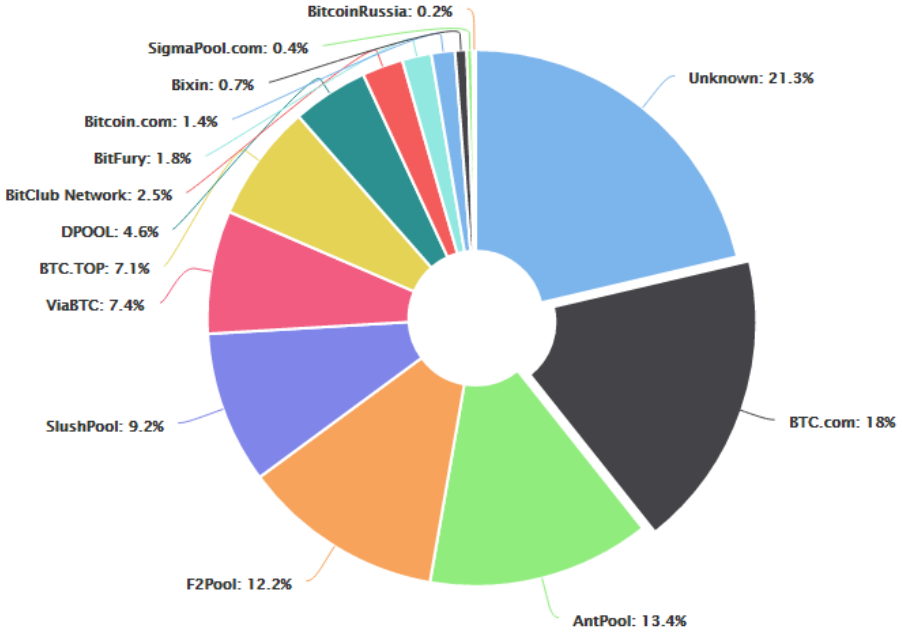


Figura 3: Pools de mineração
Fonte: https://www.blockchain.com/pools

A figura 4 apresenta um mapa com a estimativa de concentração de nós alcançáveis de Bitcoins no mundo. Vale ressaltar que esse número é uma parte do todo uma vez que representa apenas nós com portas rastreáveis. Nem todos os nós possuem portas abertas que podem ser rastreadas, seja em razão de regras de firewalls ou porque foram configuradas para não ouvir conexões. Observa-se uma grande presença de mineradores localizados: Estados Unidos, Alemanha, França e Canadá.

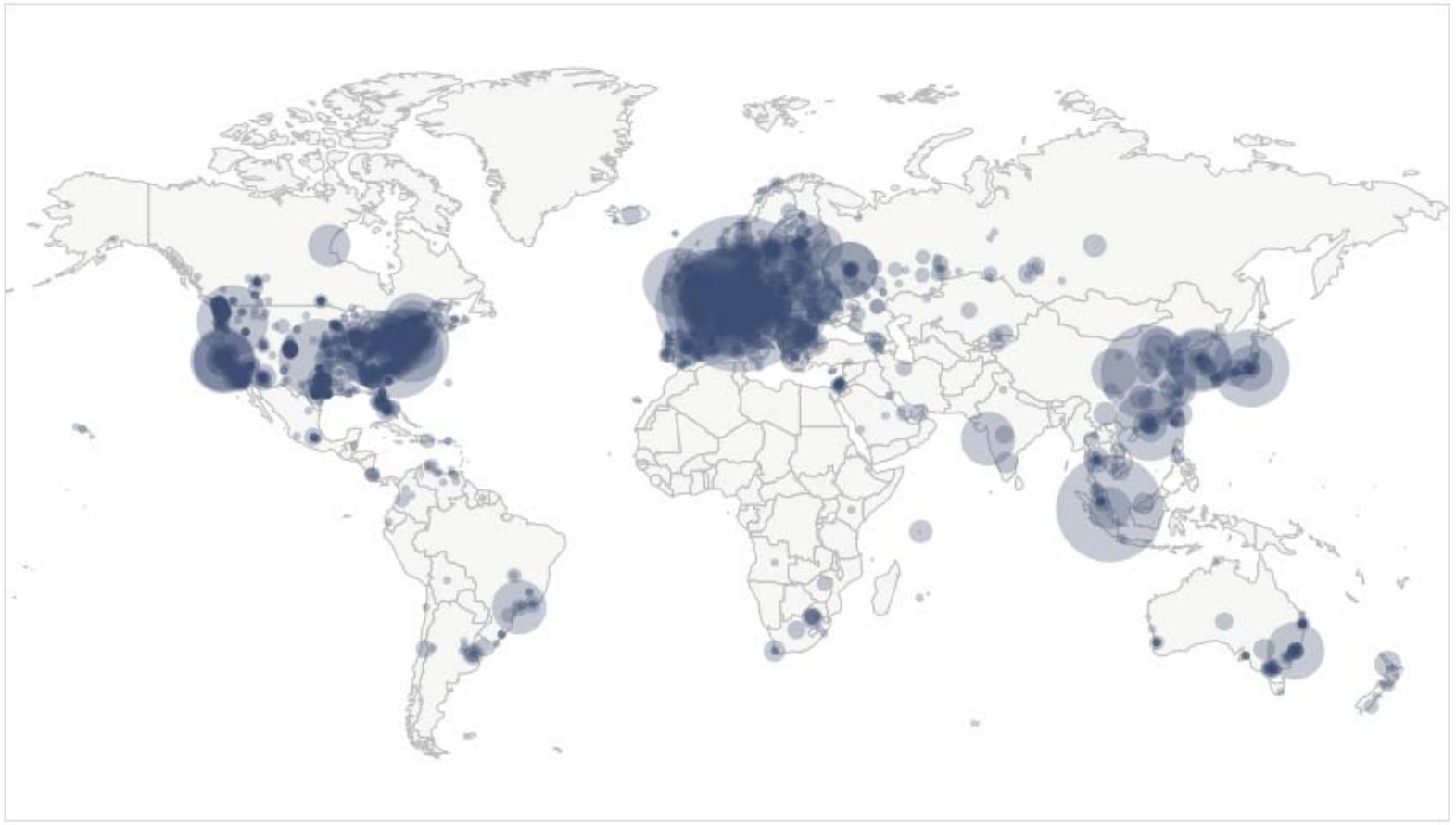


Figura 4: Nós alcançáveis de Bitcoin
Fonte: https://bitnodes.earn.com/

Os dados acima, fornecem insumos para as seguintes hipóteses:

- Fornecimento de energia com valor diferenciado, em razão o alto consumo das mineradoras;
- Utilização de outras fontes energéticas na mineração
- Existência de mineração ilegal

2.4. Simulação de Monte Carlo

O processo de modelagem de projeções e avaliações de investimentos não deve basear-se em simples intuições, mas sim em conhecimento do mercado, no entendimento das principais premissas macroeconômicas e da empresa (COSTA, COSTA, ALVIM, 2010). Neste sentido, avaliação tradicional de Fluxo de Caixa Descontado é método que reduz a intuição, uma vez que as variáveis envolvidas no problema são modeladas visando obter o valor esperado do projeto. Porém esse modelo apresenta limitações, uma vez que se trata de uma análise determinística, a qual as variáveis passíveis de riscos, são modeladas segundo a ótica do avaliador. Outro método utilizado para produzir análises com maior amplitude é através da avaliação de diferentes cenários (pessimista, esperado e otimista), o qual o risco é medido de forma mais abrangente. Para tal, modificam-se as variáveis que possuem grau de incerteza, visando a construção, baseada no mesmo modelo, de diferentes resultados. Todavia, face à alta volatilidade do valor da criptomoeda e do nível de dificuldade da rede é complexo efetuar uma estimativa dessas variáveis. Principalmente pelo fato que os valores ocorrem em tempo contínuo e constituem uma série temporal não estacionária, ou seja, o valor esperado da variável aleatória pode crescer sem limite e sua variância σ^2 (FAN, 2000).

Na literatura voltada para a modelagem de incertezas por processos estocásticos a simulação Monte Carlo é frequentemente utilizada como método matemático de geração de valores aleatórios, com o objetivo de criar amostras e mapear probabilisticamente as variáveis que afetam o modelo e consequentemente o resultado do fluxo de caixa. Para tal, são gerados valores aleatórios obtidos da função de distribuição de cada variável com grau de incerteza. No modelo serão abordadas três variáveis de incerteza: O valor da venda dos equipamentos de mineração ao final da operação – Modelado por uma distribuição continua uniforme; A projeção do valor do Bitcoin e do nível de dificuldade da rede – Modeladas pelo Movimento Geométrico Browniano (MGB),

método constantemente utilizado para variáveis de natureza contínua e não estacionária.

O processo estocástico movimento geométrico browniano pode ser descrito pela equação, na qual, a constante μ representa a tendência (drift), enquanto σ representa a volatilidade (PADDOCK, *et al*., 1988).

MGB: dp= μPdt+ σPdz

onde dz = $\Sigma\sqrt{dt}$ Σnn(0,1)

Discretização do MGB

$$P_t = P_{t-\Delta t}\, \mathrm{Exp}\left(\left(\mu - \frac{\sigma^2}{2}\right)\Delta t + \sigma\, N\,(0,1)\sqrt{\Delta t}\right)$$

3
Metodologia

Este capítulo pretende informar sobre as diversas decisões acerca da forma como este estudo foi realizado. Está dividido em seis seções que informam, respectivamente, sobre o tipo de estudo realizado, sobre o universo do estudo e processos de amostragem empreendidos, sobre os critérios de seleção de sujeitos que compõe a amostra. Na sequência, informa-se sobre os processos de coleta de dados realizados e sua justificativa, sobre os procedimentos de tratamento dos dados coletado e, por fim, sobre as possíveis repercussões que as decisões sobre como realizar o estudo impuseram aos resultados assim obtidos.

3.1.
Tipo de pesquisa

A classificação dessa pesquisa está referenciada à taxonomia proposta por Vergara (1997), na qual a pesquisa é definida quanto aos fins e meios. Tendo em vista que este trabalho visa propor, simular e analisar resultados de um modelo de fluxo de caixa descontado baseado em métodos estocásticos, trata-se de uma pesquisa aplicada quanto aos fins, já que possui finalidade prática de resolução de um problema concreto. No que concerne aos meios, em virtude da manipulação de variáveis independentes, seguida da análise dos resultados, esta pesquisa é classificada como experimental.

3.2.
Procedimentos e instrumentos de coleta de dados

Os dados foram extraídos da própria Blockchain do Bitcoin, através do site Blockchain.com, que é um serviço web explorador de blocos, que fornece gráficos de dados, estatísticas, informações de mercado do Bitcoin, APIs para desenvolvedores e permite baixar arquivos com as séries históricas registradas na Blockchain. Este trabalho utilizou toda série histórica até o presente momento em que esta pesquisa foi escrita, que compreende o período desde 03 de janeiro de 2009 até 25 de fevereiro de 2019. O download dos dados foi obtido através

da navegação no menu superior do site, clicando em Data e posteriormente no submenu Charts, que direciona para a página Blockchain Chartsm dividida em 5 grupos: Currency Statistics, Block Details, Mining Information, Network Activity E Wallet Activity.

No primeiro grupo, Currency Statistics, ao clicar em Market Price (USD) é exibido um gráfico com o preço de mercado do Bitcoin no último ano. Na parte inferior esquerda do gráfico, ao clicar no botão “all Time” é exibida toda série histórica, que pode ser baixada em arquivo ao clicar no botão “CSV”, localizado à direita da página. No grupo “Mining Information” foram obtidas as informações de Hashrate, distribuição do hashrate, dificuldade e recompensa com mineração. O processo de extração foi o mesmo descrito acima, ao selecionar os botões “all time”, para exibir toda série e posteriormente botão “CSV”, para baixar o arquivo com a referida informação.

As informações referentes às máquinas de mineração foram obtidas do site cryptocompare.com, que é um dos sites mais populares e utilizados pelos mineradores. A CryptoCompare é um provedor global de dados de mercado em criptomoedas, que oferece informações confiáveis, de alta qualidade e em tempo real sobre: preços de mercado, equipamentos, pools de mineração, além de calculadoras para analisar o retorno obtido com mineração de criptomoedas dado algumas variáveis de entrada tais como:.Hashing Power, Power Consumption, cost per KWh e pool fee.

Os dados técnicos dos equipamentos foram obtidos ao clicar no menu superior Mining e posteriormente no submenu Equipment, que abriu uma página de pesquisa com equipamentos de mineração. No menu a direita, no filtro de busca, foram selecionados Bitcoin no campo currency e ASIC no campo type . A página mostra uma lista de equipamentos ordenados por payback period. Ao clicar nos itens é possível ver todo detalhamento com informações sobre o produto.

As informações a respeito do funcionamento da Blockchain e do Bitcoin foram obtidas nos sites bitcoin.org, que foi o domínio registrado por Satoshi Nakamoto em 18 de agosto de 2018 e contêm informações, documentos, APIs a respeito da criptomoeda e no site https://github.com/bitcoin/bitcoin/tree/master/src, que contém o código fonte do Bitcoin.

3.3. Limitações

Tendo em vista que a Blockchain do Bitcoin é uma rede pública e compartilhada, não foram encontradas limitações à pesquisa

3.4. Premissas

- *Taxa de remuneração de mineração*: Para projeção do fluxo de caixa optou-se pelo suprimento desta variável em virtude da baixa representatividade na receita atual. Contudo é notório que esta variável é representativa em períodos de elevadas altas e quedas do preço do Bitcoin, conforme ocorreu no ano de 2007 até janeiro de 2018;
- *Estratégias condicionais*: O modelo não contempla condicionantes para aguardar a realização das criptomoedas para moeda FIAT, no caso de uma cotação baixa no mês. Todavia é sabido que uma das principais estratégias dos mineradores é guardar as criptomoedas em carteiras, objetivando uma realização futura, com maior valor de cambio;
- *Riscos sistêmicos*: Não foram modelados os riscos sistêmicos, devido à complexidade de estimar sua ocorrência e a projeção do impacto no mercado de mineração. Entre os possíveis riscos, destacam-se , mas não se limitam à: riscos relacionados à mudança do protocolo de consenso, possíveis restrições aos equipamentos ASIC, o surgimento de máquinas quânticas, o ataque de 51%, regulamentações e ataques cibernéticos;
- *Riscos gerais*: Por não ser objeto principal desta pesquisa, riscos inerentes à operação não foram contemplados no modelo, destacando-se, mas não se limitando à: falhas de hardware, quedas de energia, desconexões de rede, ineficiência energética, problemas alfandegários com a importação, sinistro e crime cibernético.

3.5. Modelo base de retorno com mineração

Receita

A receita de Bitcoins vem da atividade de mineração propriamente dita, que consiste na probabilidade de uma máquina resolver o desafio criptográfico que é a chave do bloco. Hayes (2015) aplicou um modelo para determinar o

número esperado de moedas de criptomoedas a serem mineradas por dia, em média, dada a dificuldade e a recompensa em bloco (número de moedas emitidas por tentativa de mineração bem-sucedida) por unidade de poder de hashing.

$$BTC/day^* = [(\beta \cdot \rho)/(\delta \cdot 2^{32})/sechr] \cdot hrday$$

Onde BTC * / dia é a quantidade esperada de bitcoins que um minerador pode esperar ganhar por dia, β é a recompensa de bloco, ρ é o poder de hashing empregado por um mineiro, e δ é a dificuldade. A constante Sechr é o número de segundos em uma hora, 3.600. A constante hrday é o número de horas em um dia, 24. A constante 2^{32} é a probabilidade normalizada de um único hash resolver um bloco e é uma função do algoritmo bitcoin. O valor para ρ, para os fins deste artigo, será dado em uma unidade padrão de 1.000 GigaHashes por segundo (GH/ s) de potência de mineração (ou equivalentemente 1 TeraHash por segundo, (TH / s)), de modo que ρ = 1.000 x 10^9. A recompensa em bloco por bitcoin é dada a 12,5 bitcoins por bloco, atualmente e passará para 6,25 a partir de maio de 2020 e será reajustada para 50% do seu valor a cada 21.000 blocos.

As constantes que normalizam o espaço dimensional para o tempo diário e para o algoritmo de mineração podem ser resumidas pelo termo θ, que será igual a:

$$\theta = 24 \text{ horas} \cdot 3600s \qquad \text{Equação (1)}$$

Pode então ser reescrita para cálculo mensal considerando Q o número de mineradoras:

$$BTC_{month} = (\theta \cdot \beta \cdot \rho \cdot Q) / (\delta \cdot 2^{32}) \cdot 30 \qquad \text{Equação (2)}$$

Por exemplo, o número de bitcoins que se pode esperar por mês empregando 44 TH / se com uma dificuldade de 6.071.846.049.920 seria calculado com a equação (2) como:

$$\frac{8640 \times 12{,}5 \times 440000000000000 \times 1}{2^{32} \times 6071846049920} \times 30$$

Resultando em 0,054665972 BTC * / mês.

O trabalho de Rosenfield (2011) se propõe a compreender os aspectos da rentabilidade por mineração em pools. O trabalho concluiu que, por causa da alta variância nas recompensas da mineração individual, a necessidade de mineração em pools se faz importante e não pode ser desconsiderada.

A receita para o minerador será o valor obtido pela equação 2, subtraído do percentual de pagamento ao pool de mineração e multiplicado pelo preço de mercado do Bitcoin (BTCPrice)

$$R_{mining} = (BTC_{month} – (BTC_{month} . P\%pool)) . BTCPrice \qquad \text{Equação (3)}$$

Custos

A atividade de mineração possui custos fixos afundados, relacionados à aquisição, instalação e manutenção dos equipamentos, além dos gastos relativos à infraestrutura necessária para operacionalização. Outro custo, de classe semi-variável, é relativo à manutenção e refrigeração, que dependendo da quantidade de máquinas, será representativo no custo total. No modelo proposto este custo foi expressado como 10% do consumo total das mineradoras. Mas sabe-se que o custo com resfriamento pode variar em razão da tecnologia dos equipamentos, da técnica de climatização, do clima local e do custo da energia. Existe ainda outros custos fixos, de menor valor, tais como aluguel, comunicação, monitoramento e manutenção. Entretanto, o maior custo desta atividade está relacionado ao consumo de energia das máquinas de mineração.

De acordo com Hayes (2015), o custo do consumo energético dos equipamentos de mineração por dia, Eday pode ser expresso como:

$$Eday = (\text{preço por kWh} \cdot 24 \text{ horas} \cdot W \text{ por GH / s}) (GH / 1.000) \qquad \text{Equação (4)}$$

Pode então ser reescrita:

$$C_{month} = (W/h \cdot Q / 1000) \cdot \text{ preço por kWh} \cdot 24 \text{ horas} \cdot 30 \text{ dias} \qquad \text{Equação (5)}$$

Por exemplo, consumo que pode se esperar por mês de um equipamento que consome 1980kWh com custo de energia 0,13 kWh seria calculado com a equação (4) como:

$$\frac{1980 \times 1}{1000} \times 0{,}13 \times 24 \times 30$$

Resultando em 185,33 mês.

O custo com refrigeração é expresso no modelo como um valor percentual do consumo dos equipamentos de mineração

$C_{cooling}$ = Emonth * P%consumo Equação (6)

O custo variável pode ser expresso como:

$C_{var} = C_{month} * C_{cooling}$ Equação (7)

O custo operacional pode ser expresso como:

$C_{op} = C_{var} + \sum Custos\ fixos$ Equação (8)

O custo de produção do Bitcoin pode ser expresso como:

$\frac{c_F + cv}{B}$ Equação (9)

Onde: CF = Custo Fixo; CV =Custo Variável; B = Bitcoins produzidos

3.6. Fluxo de caixa determinístico

O fluxo de caixa livre (FCL) é o lucro antes de juros e imposto de renda (LAJIR) abatido de imposto de renda para pessoa jurídica (IRPJ) somada à depreciação e subtraído dos investimentos. O cálculo do LAJIR é igual a receita líquida subtraída dos custos operação e manutenção (OPEX) e depreciação. O grupo de custos variáveis compreende os gastos do consumo elétrico oriundo dos equipamentos de mineração e de refrigeração do ambiente. O grupo de custos fixos possui gastos relacionados ao aluguel, comunicação com Internet de banda larga e manutenção em geral, que compreende limpeza, conservação e segurança. O fluxo de caixa compreende um período de 24 meses, onde os três primeiros meses são para montagem da operação e importação dos equipamentos; A operação ocorre efetivamente entre os 4º. e 23º meses. No 24º mês está prevista desmobilização da equipe, venda dos equipamentos e encerramento da operação. O período de 24 meses foi escolhido em razão do tempo de vida útil do equipamento uma vez que a partir do segundo ano o equipamento pode apresentar problemas por estar operando 24x7x365 e também em função do incremento do nível de dificuldade que diminui a chance de mineração dos equipamentos mais antigos.

	Mês 1-3	Mês 4-23	Mês 24
RECEITAS			
(-)CUSTOS OPERACIONAIS	**Investimento + Montagem operação**	**Operação**	**Encerramento operação**
Custos Variáveis			
Consumo mineração			
Consumo refrigeração			
Custos Fixos			
Aluguel			
Comunicação			
Manutenção			
(-) Depreciação			
LAJIR			
(-) Alíquota IRPJ:			
Lucro Líquido			
(+) Depreciação			
Investimento			
Investimento equipamento			
Investimento infraestrutura			
(+) Receita com venda de ativo			
FCL			

Parâmetros do modelo

Parâmetro	Descrição	Valor
Valor_BTC	Valor do Bitcoin	US$ 4.000
Dificulty	Taxa de dificuldade da rede	6071846049920
Custo de energia (w/h)	Custo da energia local	US$ 0,13
Hashing power	Poder de processamento do equipamento de mineração	4400000000000 00 (44TH/s)
Consumo (w/h)	Consumo da mineradora	1.980w/h
Preço US$	Preço da mineradora	US$ 2.500
%Pool_fee	Percentual que será pago ao pool de mineração. O valor é em média em torno de 2%, embora seja descrito nas regras de adesão do pool selecionado	2%
QTD_Maquinas	Quantidade de mineradoras	100
Tempo Setup (meses)	Tempo que levará para início da operação, contemplando importação e adequação do local para a atividade destinada	3
%Refrigeração	Percentual do gasto com refrigeração. Este valor é um percentual relativo ao consumo de mineração	10%
Infraestrutura US$	Investimento em infraestrutura	US$ 9.000
Periféricos US$	Investimento em periféricos	
Aluguel US$	Custo com aluguel do galpão para operação	US$ 1.300
Comunicação US$	Custo com internet	US$ 100
Manutenção US$	Custos com manutenção e conservação do local e dos equipamentos	US$ 600

Taxa de desconto (mês)	Taxa de desconto do investimento	1%a.m.
Taxa de importação	Taxa de importação dos equipamentos de mineração	75%
% preço de venda	Percentual do preço de venda do equipamento ao final da operação	33% do valor de compra

Tabela 1: Parâmetros do modelo
Fonte: Elaboração própria

3.7. Modelagem de incertezas com funções estocásticas

A análise de fluxo de caixa descontado possui limitações para modelar incertezas, que podem afetar o retorno do investimento. Em projetos de mineração de criptomoedas as principais variáveis de risco são: o nível de dificuldade da rede e o valor do Bitcoin. Desta forma, esta seção busca modelar essas variáveis de forma estocástica, utilizando o Movimento Geométrico Browniano (MGB) como padrão de comportamento, onde foram realizadas diversas simulações para estimar o nível de risco do investimento.

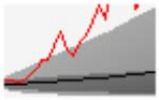
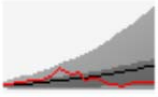
Parâmetro	**Representação gráfica**	**Função de distribuição**
Valor_BTC		MGB , sendo: $S_t = S_0 \exp\left(\left(\mu - \frac{\sigma^2}{2}\right)t + \sigma W_t\right).$ S0 : Valor inicial BTC μ: retorno σ: volatilidade
Network rate		MGB , sendo: $S_t = S_0 \exp\left(\left(\mu - \frac{\sigma^2}{2}\right)t + \sigma W_t\right).$ S0 : Valor inicial Network rate μ: retorno σ: volatilidade
preço de venda		Distribuição uniforme , sendo: mínimo: 20% máximo: 50% Valor estático: 33%

Tabela 2: Parâmetros estocásticos
Fonte: Elaboração própria

Os parâmetros de retorno (μ) e volatilidade (σ) do Bitcoin e do nível de dificuldade foram obtidos pela série histórica, conforme descrito no item 3.2. e estão representados em equivalentes mensais para os períodos representados na tabela 3. O retorno foi obtido através da média total das diferenças percentuais dos registros cronologicamente ordenados. Tendo em vista que o dado extraído apresenta os valores a cada dois dias, para obtenção do valor equivalente mensal o número resultante foi multiplicado pela raiz de quinze. A volatilidade foi obtida de forma similar ao retorno, porém a fórmula utilizada para resultante desta variável foi o desvio padrão ao invés da média.

Período	**Variável analisada**	**Retorno**	**Volatilidade**
Série histórica 03/01/09 à 04/03/19	Bitcoin	3,60% a.m.	34,61% a.m.
	Dificuldade da rede	7,12% a.m.	39,89% a.m.
Desde 2013 01/01/13 à 04/03/19	Bitcoin	2,86% a.m.	26,12% a.m.
	Dificuldade da rede	5,47% a.m.	19,90% a.m.
Último trimestre 01/01/13 à 01/03/19	Bitcoin	0,15% a.m.	11,08% a.m.
	Dificuldade da rede	1,02% a.m.	3,97% a.m.

Tabela 3: Volatilidade e retorno do Bitcoin e do Nível de dificuldade da rede.
Fonte: Elaboração própria

4
Aplicação e análise dos resultados

Este capítulo apresenta os principais resultados alcançados, discute suas implicações sobre o problema de pesquisa previamente selecionado.

4.1.
Análise do mercado de mineração

A figura 5 representa o custo de produção de um Bitcoin em 24 países, com base nas tarifas de energia elétrica divulgadas no relatório da Statisa, para o ano de 2019, disponível em: https://www.statista.com/statistics/263492/electricity-prices-in-selected-countries/. A análise considerou apenas o consumo elétrico do equipamento de mineração, desprezando todos os demais custos envolvidos. Esta análise considerou os seguintes parâmetros: mineradora Ebang E11++ 44TH/s, com consumo de 1.908 W/h; Nível de dificuldade da rede em 6071846049920 e Network Hashrate em 43464603236. Para obter o custo de produção de 1 Bitcoin é necessário descobrir quantos Satoshi serão produzidos em 1 mês, conforme Equação 1 e dividir esse valor por 1 , para descobrir quanto meses serão necessários para produzir uma unidade de Bitcoin. Posteriormente este tempo deve ser multiplicado pelo custo de consumo do equipamento, conforme Equação 5

$$Custo\ Produção\ de\ 1\ Bitcoin = \frac{1}{Equação\ 1} \times Equação\ 5$$

Substituindo as variáveis da Equação 1 pelos parâmetros de entrada, obtém-se que a mineradora produzirá 0,054665972 BTC por mês.

Logo, resolvendo a primeira parte da equação, obtém-se que serão necessários 18,29 meses para produção de uma única unidade de Bitcoin. O custo por pais é o resultado da multiplicação tempo estimado para geração de um Bitcoin, pelo custo de energia do local. Nota-se na figura 5 grande variação do custo de produção, em razão do custo de energia elétrica de cada pais.

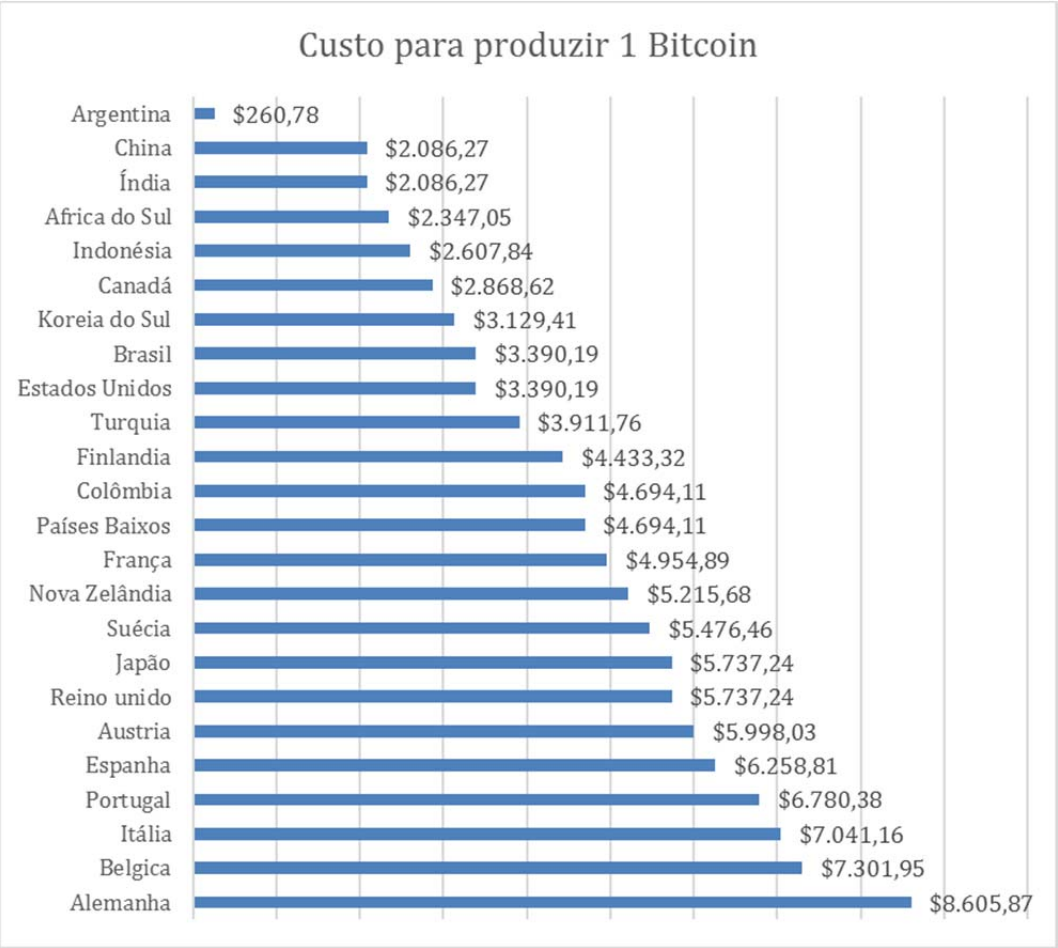


Figura 5: Custo para produzir 1 Bitcoin
Fonte: Elaboração própria

A figura 6 apresenta a relação entre custo da energia elétrica e o custo de produção de 1 Bitcoin.

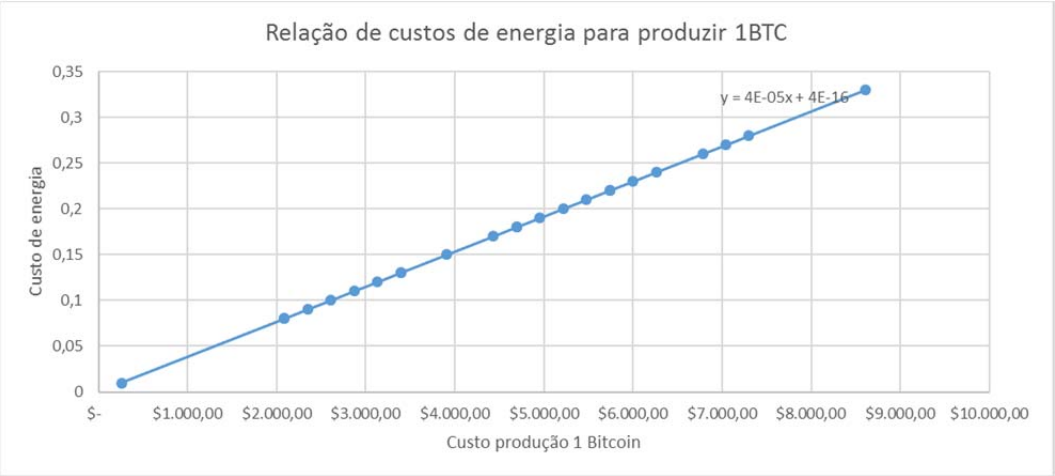


Figura 6: Correlação entre custo de energia e custo de produção BTC
Fonte: Elaboração própria

A tabela 4 apresenta os principais equipamentos de mineração (ASICs) do mercado, com seus respectivos retornos, assumindo em US$ 4.000 o valor do Bitcoin e US$0,13 o custo de energia elétrica. A coluna eficiência foi calculada pela divisão do consumo do equipamento pela capacidade de produção de Bitcoins. Observa-se uma melhoria da eficiência energética ao longo do tempo, o que reforça que o custo de produção está diminuindo em função do avanço tecnológico Rosenfield (2011). Um outro ponto que merece atenção é que, apenas uma máquina apresenta retorno positivo, considerando o custo médio de energia do Brasil, de US$0,13. Tendo em vista que o referido equipamento custa US$2.500, significa que o payback ocorrerá em aproximadamente 8 anos, desconsiderando o crescimento do nível de dificuldade da rede e demais custos operacionais.

Equipamento	Consumo w/s	Capacidade	Eficiência	Status	BTC Mês	Receita Mês	Custo Mês	Resultado(mês)	Lançamento
AntMiner S1	360	180.000	0,200%	Descontinuada	0,000223634	0,894534086	33,70	-32,80	mar/14
AntMiner S3	340	441.000	0,077%	Descontinuada	0,000547902	2,19160851	31,82	-29,63	ago/14
AntMiner S5	590	1.155.000	0,051%	Descontinuada	0,001434982	5,73992705	55,22	-49,48	fev/15
AntMiner S7	1210	4.860.000	0,025%	Descontinuada	0,006038105	24,15242032	113,26	-89,10	set/15
AntMiner S9	1375	14.000.000	0,010%	Disponível	0,017393718	69,57487334	128,70	-59,13	jul/16
AntMiner S11	1530	20.500.000	0,007%	Disponível	0,025469373	101,8774931	143,21	-41,33	ago/18
AntMiner S15	1596	28.000.000	0,006%	Disponível	0,034787437	139,1497467	149,39	-10,24	nov/18
Ebang E11++	1980	44.000.000	0,005%	Disponível	0,054665972	218,6638876	185,33	33,34	jan/19

Tabela 4: Consumo equipamentos de mineração.
Fonte: Elaboração própria

A figura 7 apresenta o desempenho ao longo do tempo das maquinas ASIC produzidas pela Antminer, principal fabricante de equipamentos de mineração de Bitcoin do Mundo. Foram avaliadas as mineradoras AntMiner S1, AntMiner S3, AntMiner S5, AntMiner S7 e AntMiner S9, considerando operação a partir das suas respectivas datas de lançamento, custo de energia de US$0,01 e dados de consumo e capacidade conforme consta na tabela 4. Foram utilizados os dados históricos o valor do Bitcoin e do nível de dificuldade do período de 2 de março de 2014 até 28 de fevereiro de 2019 para calcular a receita em mineração do período de acordo com a Equação 3 e o consumo de energia, calculado pela aplicação da Equação 2. Observa-se o tempo acelerado de obsolescência dos equipamentos, principalmente das primeiras gerações de ASIC e redução acentuada de geração de Bitcoins, acarretada pelo incremento do nível de dificuldade da rede. As mineradoras S7 e S9 tiveram o tempo de vida prolongado em razão da alta valorização da criptomoeda a partir de 2016

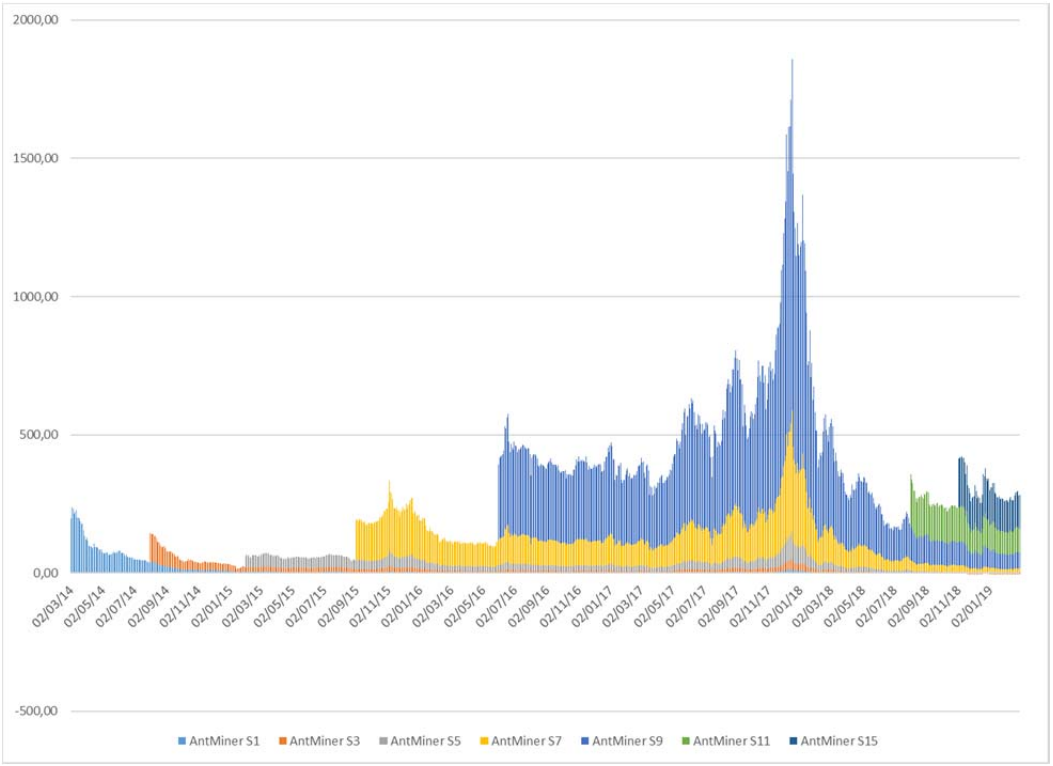


Figura 7: Receita das mineradoras no tempo
Fonte: Elaboração própria

4.2. Análise do fluxo de caixa

Com base no modelo de fluxo de caixa descrito no capítulo 3, foram avaliados o valor presente líquido - VLP e a taxa interna de retorno - TIR para um primeiro cenário, julgado como mais provável, imaginando hipoteticamente que o valor do Bitcoin permaneça estável em US$4.000. Como premissas de entrada no modelo, de acordo com tabela 1, foram considerados: Três meses para inicialização da operação; Aquisição de 100 mineradoras E11++ 44TH/s, no valor de USD$2.500; Custo fixo de US$2.000 , que compreende US$1.300 de aluguel, US$600 de manutenção e US$100 de comunicação; O custo variável , que consiste no gasto de energia dos equipamentos, com consumo individual de 1.980kW/h e custo de refrigeração igual à 10% do consumo total das mineradoras; Venda dos equipamentos à 33% do valor de compra; Dificuldade fixa da rede em 6071846049920; Custo local de energia em US$0,13; Taxa de importação de 75% e taxa de desconto 1%a.m. Após execução do modelo obteve-se resultado negativo de -9,04% para TIR e - US$408.518 para o VPL. Em seguida foi efetuada a simulação de um cenário otimista, em que o valor do Bitcoin dobra seu valor até o final do primeiro trimestre e fica mantido em US$8.000 durante toda operação. O resultado também foi negativo,

apresentando TIR: -1,89% e VPL: -US$139,08. Em função do resultado negativo para os cenários mais provável e otimista, não foi considerado o cenário pessimista. Segue abaixo alguns pontos que merecem destaque em relação ao fluxo de caixa:

- O fluxo negativo durante toda operação;
- Existe queda da receita a partir do 16º mês, acarretada pela redução da recompensa de 12,5BTC para 6,25BTC, prevista para maio 2020;
- O prejuízo nos dois cenários foi amenizado pela venda dos equipamentos ao final da operação

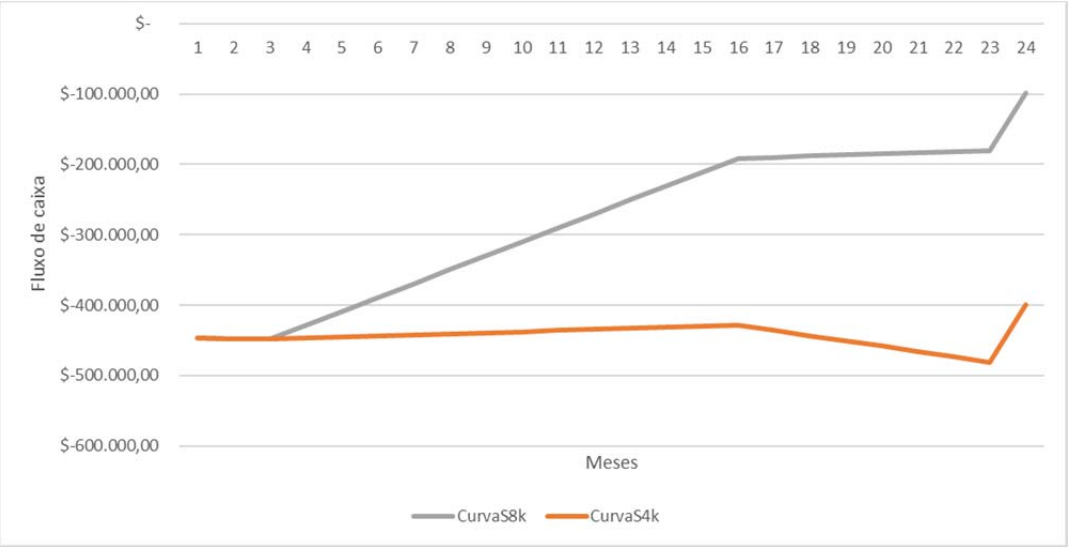


Figura 8: Fluxo de caixa – modelo determinístico
Fonte: Elaboração própria

4.3. Análise de sensibilidade

Esta seção se propõe a efetuar uma análise de sensibilidade das principais variáveis envolvidas no problema e estudar o impacto nos indicadores financeiros com resultado do investimento.

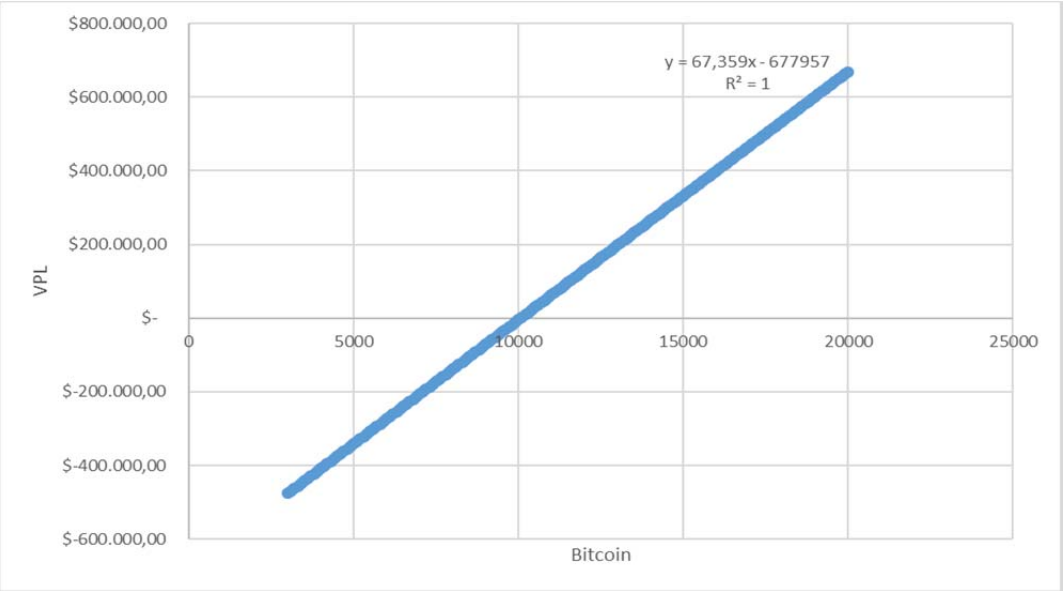


Figura 9: Sensibilidade VPL versus Valor Bitcoin
Fonte: Elaboração própria

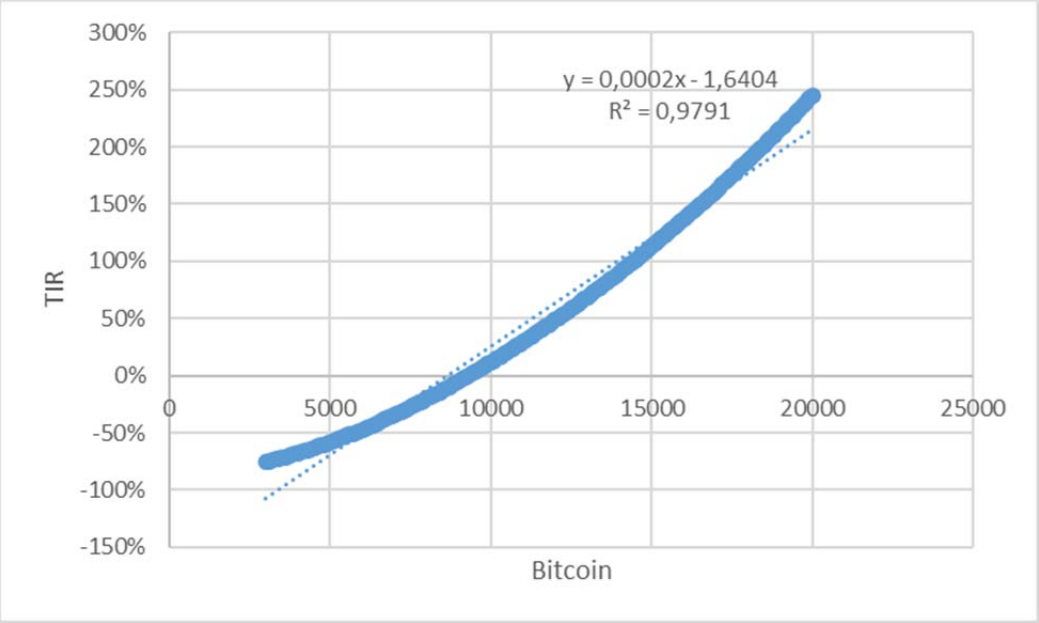


Figura 10: Sensibilidade TIR versus Valor Bitcoin
Fonte: Elaboração própria

As figuras 9 e 10 demonstram, o comportamento do VPL e da TIR em relação a variação do valor do Bitcoin. Observa-se para o VPL um crescimento linear, com função 67,359x – 677957, o que significa que para uma taxa de desconto de 12,68%a.a., o investimento passa apresentar retorno positivo apenas com cotação do Bitcoin acima de US$10.065.

Valor do Bitcoin	Custo da energia elétrica (US$ por kW/s)					
	$ 0,01	$ 0,03	$ 0,05	$ 0,08	$ 0,10	$ 0,13
$ 3.000,00	-33,19%	-42,11%	-50,58%	-62,34%	-69,43%	-78,67%
$ 4.000,00	-20,30%	-29,97%	-39,25%	-52,34%	-60,43%	-71,40%
$ 4.500,00	-13,39%	-23,41%	-33,07%	-46,78%	-55,34%	-67,11%
$ 5.000,00	-6,15%	-16,54%	-26,55%	-40,86%	-49,86%	-62,39%
$ 5.500,00	1,38%	-9,34%	-19,72%	-34,59%	-44,00%	-57,25%
$ 6.000,00	9,23%	-1,84%	-12,56%	-27,98%	-37,79%	-51,71%
$ 6.500,00	17,38%	5,98%	-5,09%	-21,03%	-31,22%	-45,77%
$ 7.000,00	25,83%	14,10%	2,70%	-13,77%	-24,32%	-39,45%
$ 7.500,00	34,58%	22,52%	10,79%	-6,19%	-17,08%	-32,78%
$ 8.000,00	43,63%	31,24%	19,18%	1,71%	-9,53%	-25,77%
$ 8.500,00	52,99%	40,27%	27,88%	9,92%	-1,66%	-18,41%
$ 9.000,00	62,64%	49,59%	36,88%	18,43%	6,52%	-10,74%
$ 9.500,00	72,59%	59,22%	46,18%	27,24%	15,01%	-2,75%
$ 10.000,00	82,85%	69,15%	55,78%	36,35%	23,80%	5,56%
$ 10.500,00	93,41%	79,38%	65,68%	45,77%	32,90%	14,17%
$ 11.000,00	104,27%	89,91%	75,89%	55,48%	42,29%	23,09%
$ 11.500,00	115,44%	100,74%	86,39%	65,50%	51,98%	32,30%
$ 12.000,00	126,92%	111,88%	97,20%	75,82%	61,98%	41,82%
$ 12.500,00	138,70%	123,33%	108,31%	86,43%	72,27%	51,63%
$ 13.000,00	150,80%	135,08%	119,73%	97,35%	82,86%	61,75%
$ 13.500,00	163,21%	147,14%	131,45%	108,58%	93,76%	72,16%
$ 14.000,00	175,93%	159,52%	143,48%	120,10%	104,96%	82,87%

Tabela 5: Sensibilidade TIR – Valor do Bitcoin versus Custo de Energia elétrica (US$ por kW/s).
Fonte: Elaboração própria

A tabela 5 mostra a variação das duas mais importantes variáveis envolvidas no processo de mineração, que são o custo da energia e o valor de mercado do Bitcoin. Observa-se que mesmo com baixo custo de energia, o investimento não é viável dada a cotação atual de US$4.000.

Os dados acima, fornecem insumos para as seguintes hipóteses:

- Os custos operacionais foram superestimados;
- O investimento está elevado, sendo possível conseguir redução do preço unitário dos equipamentos em função de compra em escala;
- Os mineradores estão operando sem realizar o lucro, apostando em um aumento futuro do valor da criptomoeda.

Quantidade de mineradoras \ Valor do Bitcoin (US$)	$ 4.000,00	$ 8.000,00	$10.000,00	$ 11.000,00	$ 12.000,00	$ 13.000,00	$ 14.000,00	$ 15.000,00
100	$ -408.518,82	$ -139.081,11	$ -4.362,25	$ 62.997,18	$130.356,61	$197.716,03	$265.075,46	$ 332.434,89
120	$ -481.127,61	$ -157.802,35	$ 3.860,28	$ 84.691,59	$165.522,91	$246.354,22	$327.185,53	$ 408.016,85
140	$ -553.736,39	$ -176.523,59	$12.082,81	$106.386,01	$200.689,21	$294.992,41	$389.295,61	$ 483.598,81
160	$ -626.345,18	$ -195.244,84	$20.305,33	$128.080,42	$235.855,51	$343.630,59	$451.405,68	$ 559.180,76
180	$ -698.953,96	$ -213.966,08	$28.527,86	$149.774,83	$271.021,81	$392.268,78	$513.515,75	$ 634.762,72
200	$ -771.562,75	$ -232.687,32	$36.750,39	$171.469,25	$306.188,11	$440.906,96	$575.625,82	$ 710.344,68
220	$ -844.171,54	$ -251.408,56	$44.972,92	$193.163,66	$341.354,41	$489.545,15	$637.735,89	$ 785.926,63
240	$ -916.780,32	$ -270.129,81	$53.195,45	$214.858,08	$376.520,71	$538.183,34	$699.845,96	$ 861.508,59
260	$ -989.389,11	$ -288.851,05	$61.417,98	$236.552,49	$411.687,01	$586.821,52	$761.956,04	$ 937.090,55
280	$ -1.061.997,89	$ -307.572,29	$69.640,51	$258.246,91	$446.853,31	$635.459,71	$824.066,11	$ 1.012.672,51
300	$ -1.134.606,68	$ -326.293,54	$77.863,04	$279.941,32	$482.019,61	$684.097,89	$886.176,18	$ 1.088.254,46

Tabela 6: Sensibilidade VPL - Quantidade mineradoras versus Valor do Bitcoin.
Fonte: Elaboração própria

A tabela 6 mostra a variação da VPL em relação ao valor do Bitcoin e a quantidade de máquinas em operação. Considerando que a infraestrutura suportaria ampliação de até 3 vezes a capacidade planejada para 100 máquinas, observa-se que a quantidade de máquinas altera significativamente o retorno do investimento, principalmente em US$ 10.000, que é o ponto de inflexão para as premissas utilizadas.

% Crescimento da Dificuldade \ Valor do Bitcoin	$10.000,00	$12.000,00	$13.000,00	$14.000,00	$15.000,00
0%	11,56%	48,46%	68,70%	90,15%	112,80%
0,05%	10,63%	47,26%	67,36%	88,66%	111,16%
0,10%	9,70%	46,07%	66,03%	87,18%	109,53%
0,15%	8,79%	44,89%	64,71%	85,72%	107,91%
0,30%	6,07%	41,39%	60,80%	81,38%	103,12%
0,50%	2,54%	36,84%	55,71%	75,73%	96,89%
0,75%	-1,72%	31,34%	49,55%	68,88%	89,33%
1,00%	-5,83%	26,03%	43,61%	62,28%	82,04%
1,25%	-9,77%	20,91%	37,87%	55,89%	74,98%
1,50%	-13,57%	15,97%	32,33%	49,73%	68,17%
1,75%	-17,22%	11,21%	26,98%	43,78%	61,59%
2,00%	-20,73%	6,62%	21,82%	38,03%	55,23%

Tabela 7: Sensibilidade TIR para Taxa de crescimento Dificuldade versus Valor do Bitcoin.
Fonte: Elaboração própria

A tabela 7 ilustra a variação da TIR de acordo com diferentes combinações entre o preço do Bitcoin e o nível de dificuldade, representado por uma taxa mensal de crescimento. Nota-se a forte influência desta variável no resultado, que é responsável pela depreciação do equipamento e com isso possui a capacidade de reduzir drasticamente o retorno do investimento, dependendo da taxa de crescimento.

A tabela 8 ilustra a variação do VPL, de acordo com o incremento do custo de refrigeração do ambiente, que é representado no modelo como um percentual do consumo dos equipamentos. Observa-se que quanto maior o gasto com refrigeração, menor será o retorno do investimento. Isso ocorre, pois, esta variável impacta no custo operacional. Este resultado corrobora com o movimento de centralização das fazendas de minerações em locais com o clima muito baixo, pela busca de técnicas, mais econômicas, de resfriamento, bem como em locais com menor preço de energia.

%Consumo	VPL
0,00%	$ -382.795,60
1,00%	$ -385.367,93
5,00%	$ -395.657,21
10,00%	$ -408.518,82
20,00%	$ -434.242,04
30,00%	$ -459.965,26
40,00%	$ -485.688,48
50,00%	$ -511.411,70
60,00%	$ -537.134,92
70,00%	$ -562.858,13
80,00%	$ -588.581,35
90,00%	$ -614.304,57
100,00%	$ -640.027,79

Tabela 8: Sensibilidade VPL para %Incremento do consumo de refrigeração
Fonte: Elaboração própria

A tabela 9 demonstra a variação do VPL, de acordo com a taxa de importação. Nota-se que quanto mais elevado o imposto, maior será o investimento, que consequentemente impactará negativamente o retorno do investimento

%imposto	VPL
0,00%	$ -221.018,82
1,00%	$ -223.518,82
5,00%	$ -233.518,82
10,00%	$ -246.018,82
20,00%	$ -271.018,82
30,00%	$ -296.018,82
40,00%	$ -321.018,82
50,00%	$ -346.018,82
60,00%	$ -371.018,82
70,00%	$ -396.018,82
80,00%	$ -421.018,82
90,00%	$ -446.018,82
100,00%	$ -471.018,82

Tabela 9: Sensibilidade VPL para %Imposto de importação
Fonte: Elaboração própria

A tabela 10 apresenta a sensibilidade da TIR em função da variação do custo do equipamento e de energia elétrica. Nota-se que dependendo do valor do equipamento, não será viável o investimento mesmo com custo zero de energia. Embora pareça incongruente é justificável observando os dados da Tabela 4, que indicam que a mineradora produz US$33,34 por mês. Portanto não é possível recuperar em 20 meses um valor elevado de investimento, considerando cotação do Bitcoin próxima a US$4.000.

Custo unitário da mineradora	Custo da eletricidade (kW/s)					
	$ -	$ 0,01	$ 0,03	$ 0,05	$ 0,08	$ 0,13
$2.500,00	-15,33%	-20,30%	-29,97%	-39,25%	-52,34%	-71,40%
$2.450,00	-14,38%	-19,48%	-29,38%	-38,88%	-52,28%	-71,74%
$2.400,00	-13,38%	-18,61%	-28,77%	-38,50%	-52,22%	-72,10%
$2.350,00	-12,33%	-17,70%	-28,12%	-38,10%	-52,16%	-72,47%
$2.300,00	-11,24%	-16,75%	-27,44%	-37,68%	-52,09%	-72,85%
$2.250,00	-10,08%	-15,74%	-26,73%	-37,24%	-52,03%	-73,25%
$2.200,00	-8,87%	-14,69%	-25,98%	-36,78%	-51,96%	-73,67%
$2.150,00	-7,59%	-13,58%	-25,19%	-36,29%	-51,88%	-74,11%
$2.100,00	-6,24%	-12,40%	-24,35%	-35,77%	-51,80%	-74,57%
$2.050,00	-4,81%	-11,17%	-23,47%	-35,23%	-51,72%	-75,06%
$2.000,00	-3,31%	-9,86%	-22,54%	-34,65%	-51,63%	-75,56%
$1.950,00	-1,71%	-8,47%	-21,56%	-34,05%	-51,53%	-76,09%
$1.900,00	-0,02%	-7,00%	-20,51%	-33,40%	-51,44%	-76,65%
$1.850,00	1,79%	-5,43%	-19,40%	-32,71%	-51,33%	-77,23%
$1.800,00	3,70%	-3,77%	-18,21%	-31,98%	-51,22%	-77,85%
$1.750,00	5,75%	-1,99%	-16,95%	-31,20%	-51,10%	-78,49%
$1.700,00	7,93%	-0,09%	-15,61%	-30,37%	-50,97%	-79,17%
$1.650,00	10,27%	1,94%	-14,16%	-29,48%	-50,83%	-79,89%
$1.600,00	12,78%	4,12%	-12,61%	-28,52%	-50,69%	-80,65%
$1.550,00	15,48%	6,46%	-10,95%	-27,50%	-50,53%	-81,45%
$1.500,00	18,39%	8,99%	-9,15%	-26,39%	-50,36%	-82,29%
$1.450,00	21,54%	11,72%	-7,21%	-25,19%	-50,17%	-83,18%
$1.400,00	24,95%	14,68%	-5,11%	-23,89%	-49,97%	-84,11%
$1.350,00	28,66%	17,90%	-2,82%	-22,47%	-49,75%	-85,10%
$1.300,00	32,70%	21,41%	-0,33%	-20,92%	-49,51%	-86,13%
$1.250,00	37,13%	25,25%	2,40%	-19,23%	-49,25%	#NUM!
$1.200,00	42,00%	29,47%	5,40%	-17,37%	-48,96%	#NUM!
$1.150,00	47,36%	34,12%	8,70%	-15,32%	-48,64%	#NUM!
$1.100,00	53,31%	39,27%	12,37%	-13,04%	-48,28%	#NUM!
$1.050,00	59,93%	45,01%	16,45%	-10,50%	-47,88%	#NUM!
$1.000,00	67,34%	51,43%	21,01%	-7,65%	-47,42%	#NUM!

Tabela 10: Sensibilidade TIR para Custo mineradora versus Custo eletricidade
Fonte: Elaboração própria

4.3.1.
Análise em diferentes cenários

Nesta e etapa foram efetuadas 1000 simulações, para três cenários, para calcular a probabilidade do VPL e da TIR, considerando como premissas básicas o tempo de operação de 24 meses, inicialização da operação a partir do terceiro mês, investimento até US$500.000 (quinhentos mil dólares), que compreende: Aquisição de 100 mineradoras E11++ 44TH/s, no valor de USD$2.500; Custo fixo de US$2.000, que compreende US$1.300 de aluguel, US$600 de manutenção e US$100 de comunicação; O custo variável, que consiste no gasto de energia dos equipamentos, com consumo individual de 1.980 kW/h. A venda do ativo foi representada como uma função de distribuição uniforme, com mínimo de 20% e máximo de 50%; Custo de energia em US$0,13 por kW/s; A taxa de importação em 75%; O crescimento do Bitcoin seguindo o modelo previsto pelo Movimento Geométrico Browniano(MGB), com valor inicial de US$3.863. O cenário 1 utilizou os dados históricos para cálculo do retorno (μ) em 3,6% e da volatilidade (σ) em 34,61%; O crescimento no nível de dificuldade previsto também pelo MGB, com início em 6071846049920, retorno (μ) de 7,12% e volatilidade (σ) de 39,89% também foi calculado com base na série histórica. O cenário 2 prevê os mesmos valores do cenário anterior, com exceção dos valores de retorno e volatilidade, onde foram utilizados os resultados para o último trimestre sendo: μ(BTC)=0,15% σ(BTC)=11,08% , μ(Dificulty)=2,17% σ(Dificulty)=3,91% e por fim o cenário 3 com retorno e volatilidade do trimestre

Cenário 1 – Retorno e volatilidade da série histórica – Preço do Bitcoin e Nível de dificuldade da rede

Nas figuras 11, 12 e 13 observa-se existe 70% de probabilidade do valor presente líquido ser abaixo de zero. Com 95% de confiança os resultados do VPL e da TIR ficarão respectivamente entre US$ -0,69MM e US$ 7,7MM e -85% e 2608%. Os resultados evidenciam elevadíssimo grau de risco do investimento, oriundo da volatilidade histórica das variáveis preço do Bitcoin e Dificuldade.

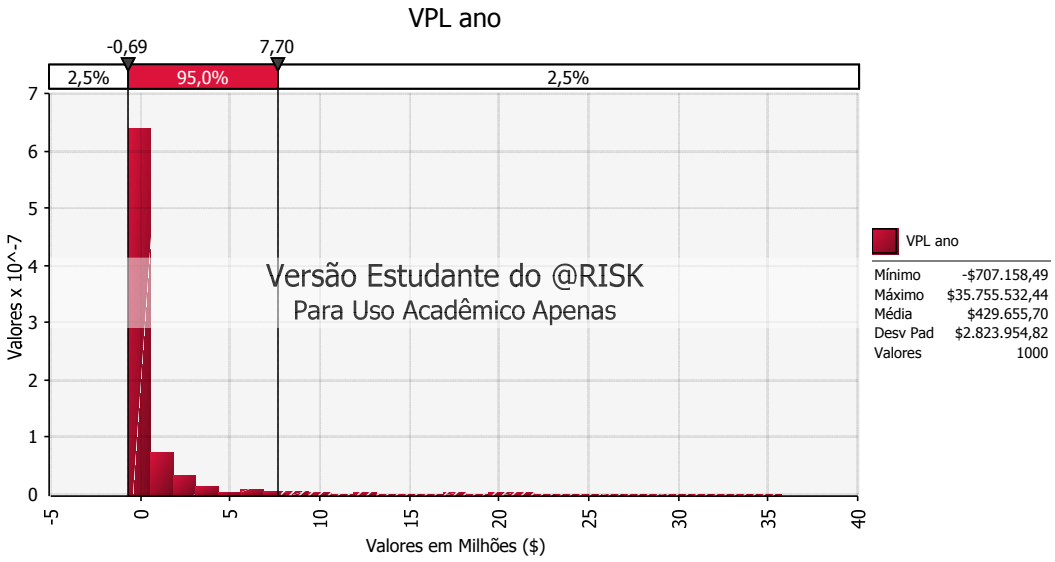


Figura 11: Probabilidade VPL com 95% confiança - Cenário 1
Fonte: Elaboração própria

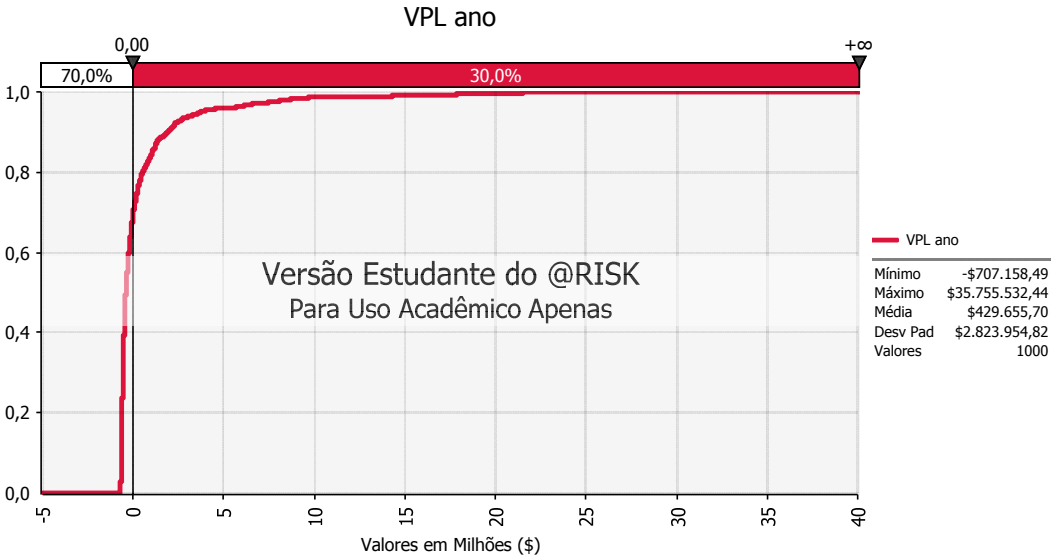


Figura 12: Probabilidade VPL positivo- Cenário 1
Fonte: Elaboração própria

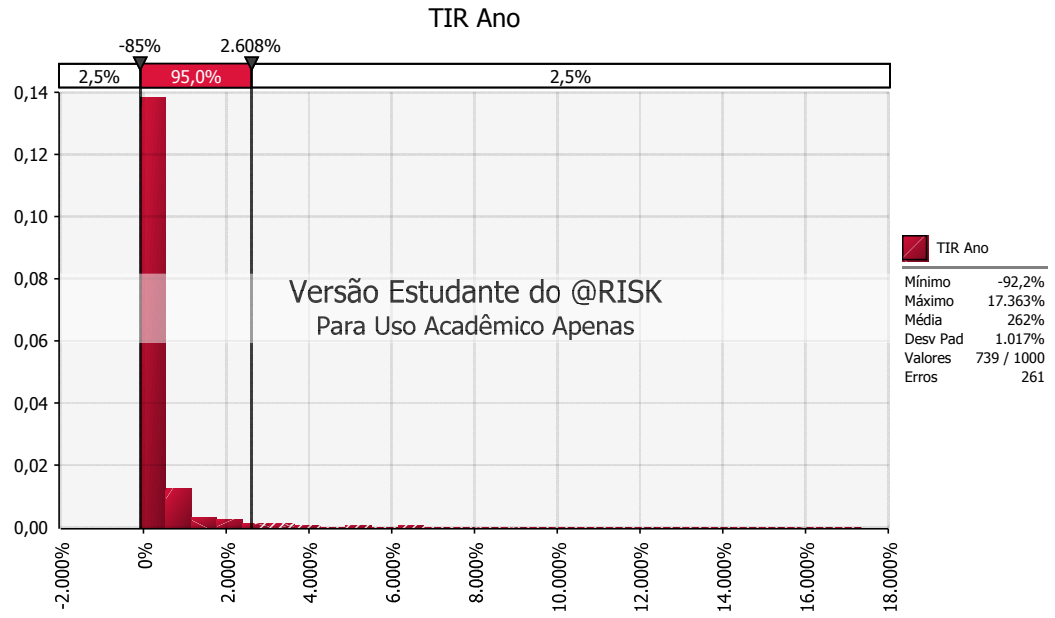


Figura 13: Probabilidade TIR com 95% confiança - Cenário 1
Fonte: Elaboração própria

Na figura 14 é exibido um gráfico de tornado, que evidencia as variáveis com maior influência nos resultados obtidos para a simulação. Os dados corroboram com a análise de sensibilidade da tabela 7 e figura 9, evidenciando que o nível de dificuldade possui efeito negativo, reduzido o resultado financeiro ao longo do tempo. O Bitcoin produzirá efeito tanto positivo quanto negativo, dependendo do valor resultante. Para uma operação pautada nas premissas do modelo, principalmente em relação ao custo operacional, não é viável o investimento enquanto a moeda estiver cotada abaixo de US$10.000

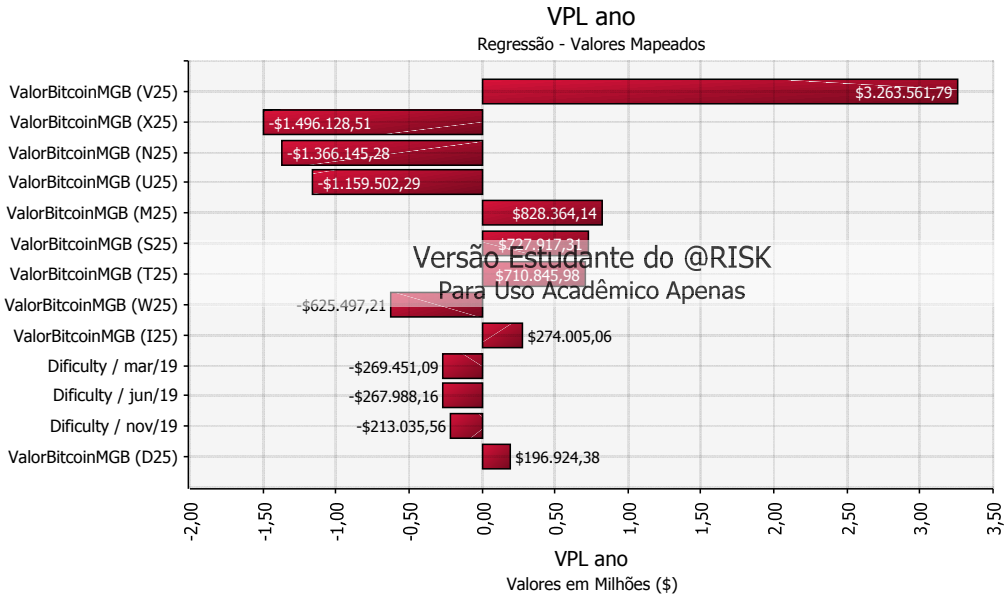


Figura 14: Graf. Tornado de sensibilidade VPL- Cenário 1
Fonte: Elaboração própria

Na figura 15 nota-se que em média o fluxo de caixa permanece próximo a zero, com crescimento da amplitude no tempo, influenciado pela incerteza do valor do Bitcoin, dada volatilidade histórica.

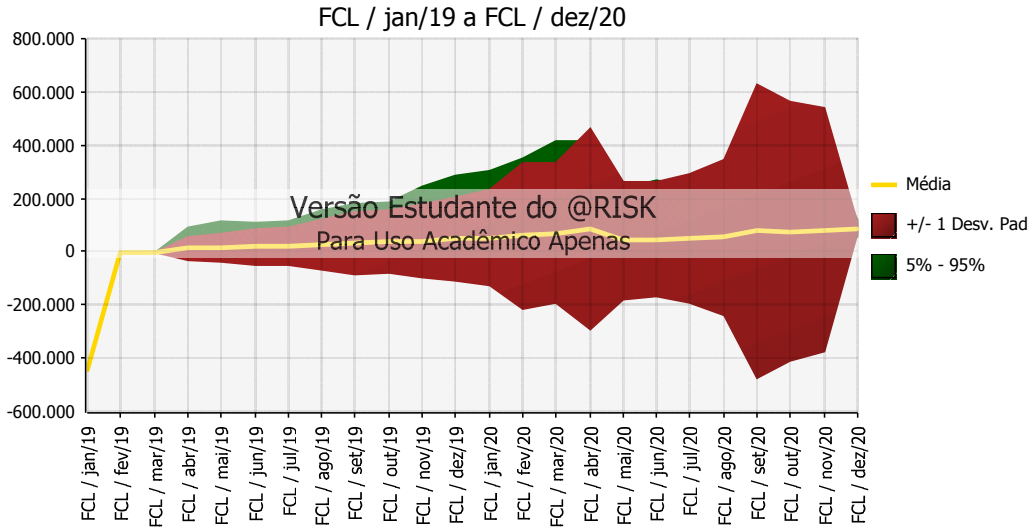


Figura 15: Fluxo de caixa- Cenário 1
Fonte: Elaboração própria

As figuras 16 e 17 estão representadas as simulações para as variáveis de incerteza em função do tempo. Nota-se que apesar da possibilidade da cotação do Bitcoin ultrapassar US$20.000, o valor se manteve abaixo de US$6.000 entre 25% e 75% dos dados simulados.

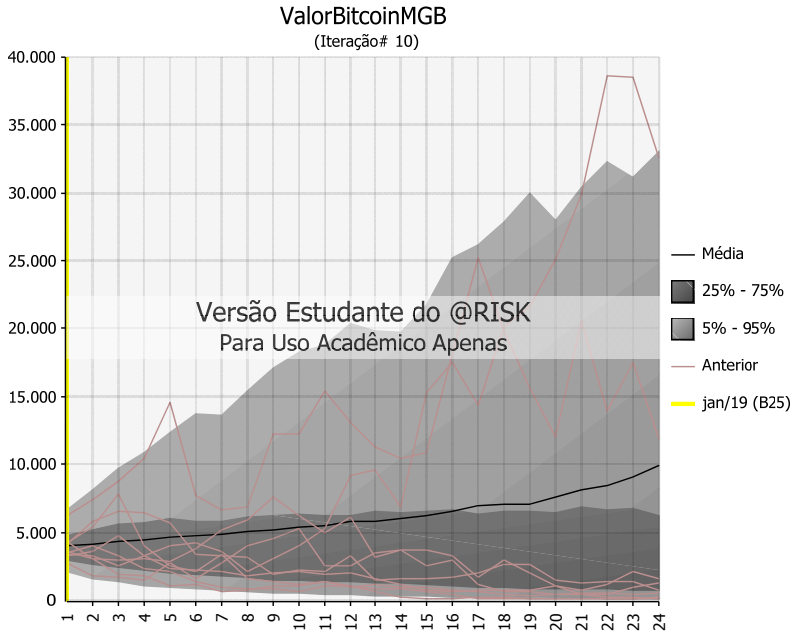


Figura 16: Simulações MGB para Bitcoin- Cenário 1
Fonte: Elaboração própria

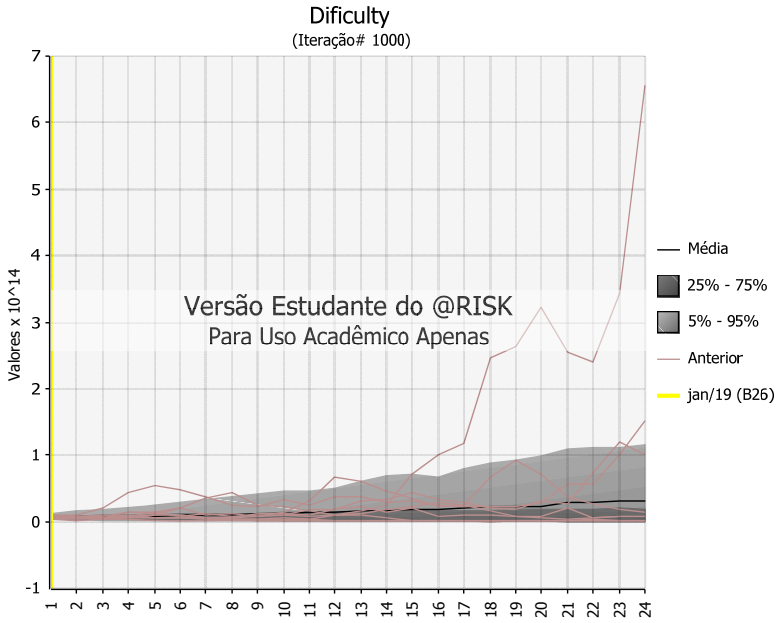


Figura 17: Simulações MGB para Dificulty- Cenário 1
Fonte: Elaboração própria

Cenário 2 – Retorno e volatilidade desde 2013 – Preço do Bitcoin e Nível de dificuldade da rede

Tendo em vista o contexto histórico, optou-se por analisar a probabilidade com base no retorno e volatilidade a partir de 2013. Nas figuras 18, 19, 20 e 21 podem ser vistos que existe 90,1% de probabilidade de que o valor presente líquido seja negativo e 77,2% da TIR estar abaixo de zero. Considerando o nível de confiança de 95%, os resultados para o VPL e a TIR ficarão respectivamente entre US$ -0,742MM e US$ 0,852MM e -86% e 309%. Embora o modelo apresente uma ínfima probabilidade de ganho colossal, nota-se eliminação de ganhos na ordem de 1000% em comparação com o cenário anterior.

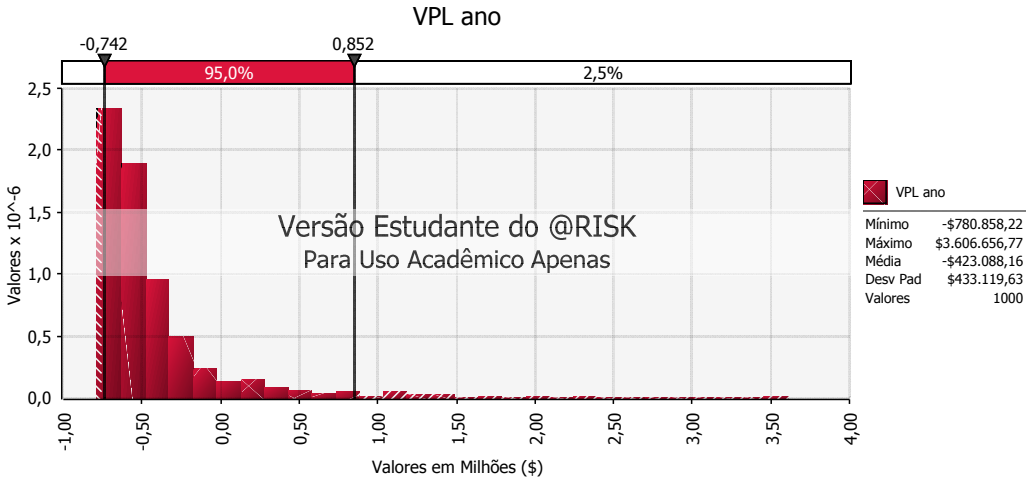


Figura 18: Probabilidade VPL com 95% de confiança- Cenário 2
Fonte: Elaboração própria

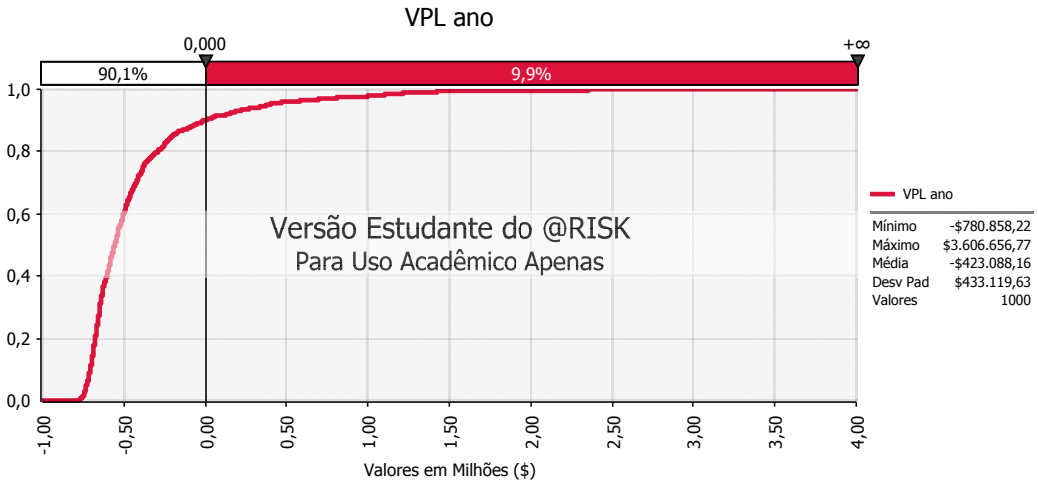


Figura 19: Probabilidade VPL positiva- Cenário 2
Fonte: Elaboração própria

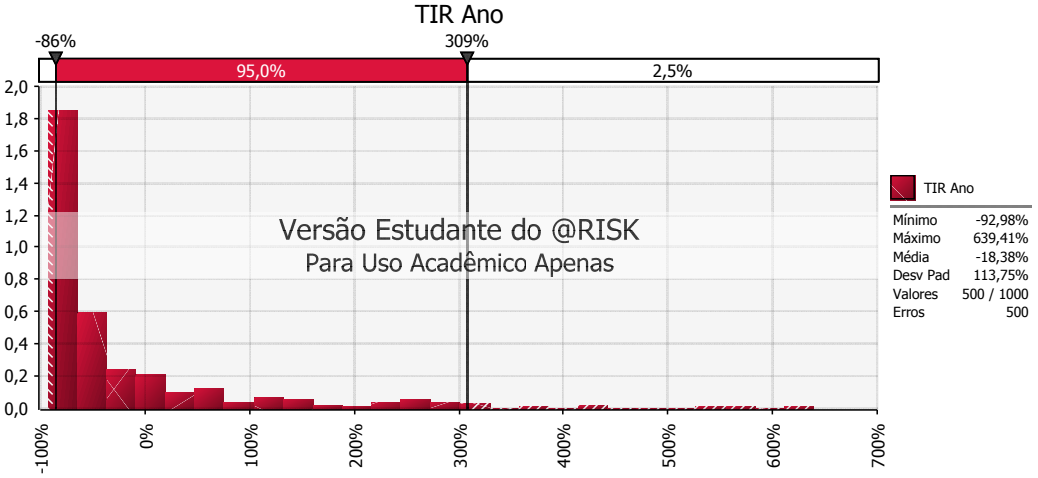


Figura 20: Probabilidade TIR com 95% de confiança- Cenário 2
Fonte: Elaboração própria

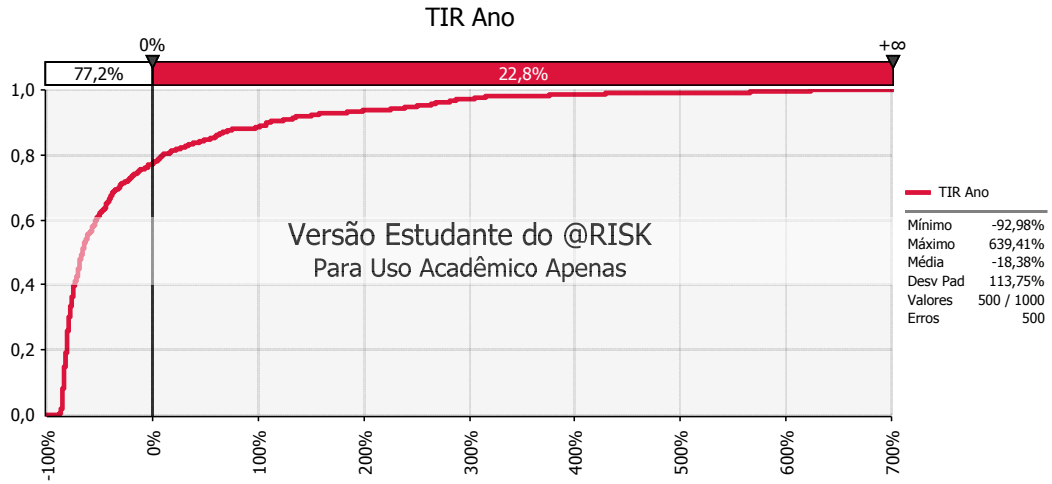


Figura 21: Probabilidade TIR positiva- Cenário 2
Fonte: Elaboração própria

Na figura 22 , observa-se redução da amplitude do resultado do fluxo de caixa , em comparação com o cenário anterior. Nota-se ainda uma elevação no último período, resultante da venda dos equipamentos ao final da operação, o que indica que os resultados positivos obtidos durante a simulação, foram resultantes primordialmente da venda.

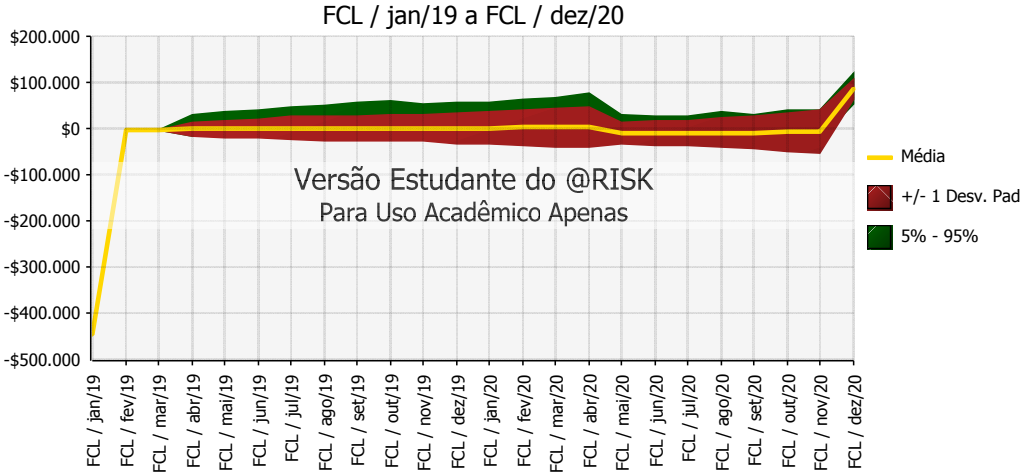


Figura 22: Fluxo de caixa- Cenário 2
Fonte: Elaboração própria

Cenário 3 – Retorno e volatilidade do último trimestre – Preço do Bitcoin e Nível de dificuldade da rede

Entendendo que o risco e a volatilidade estão diminuindo no decorrer do tempo e partindo da premissa, que o Bitcoin é de notório conhecimento, o cenário 3 explorou uma nova simulação, contemplando retorno e volatilidade do último trimestre. Nas figuras 23, 24 e 25 observa-se que não existe possibilidade,

considerando as premissas estabelecidas, do valor presente líquido ser positivo. Considerando um grau de confiança de 95%, o resultado da taxa interna de retorno será entre -85,6% e -39,3%

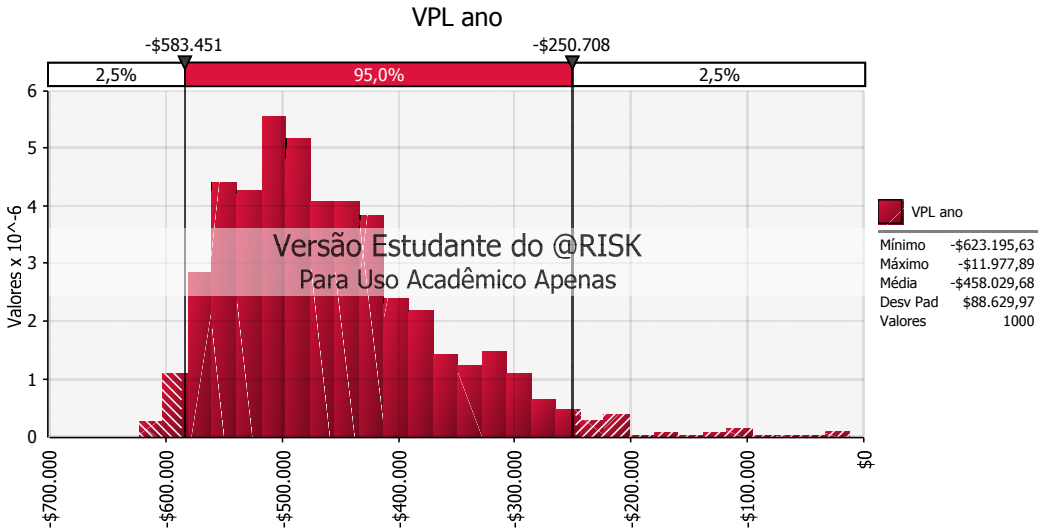


Figura 23: Probabilidade VPL com 95% de confiança- Cenário 3
Fonte: Elaboração própria

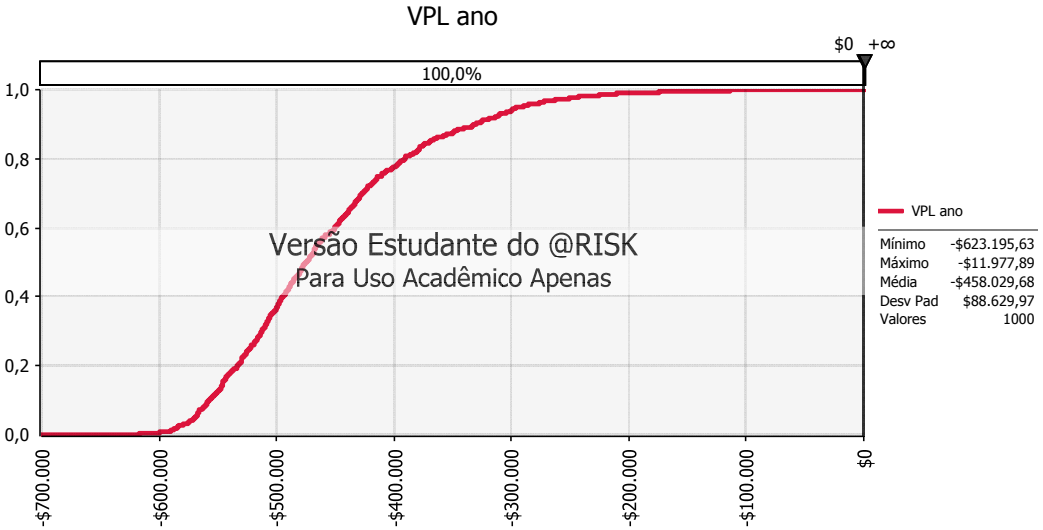


Figura 24: Probabilidade VPL positivo- Cenário 3
Fonte: Elaboração própria

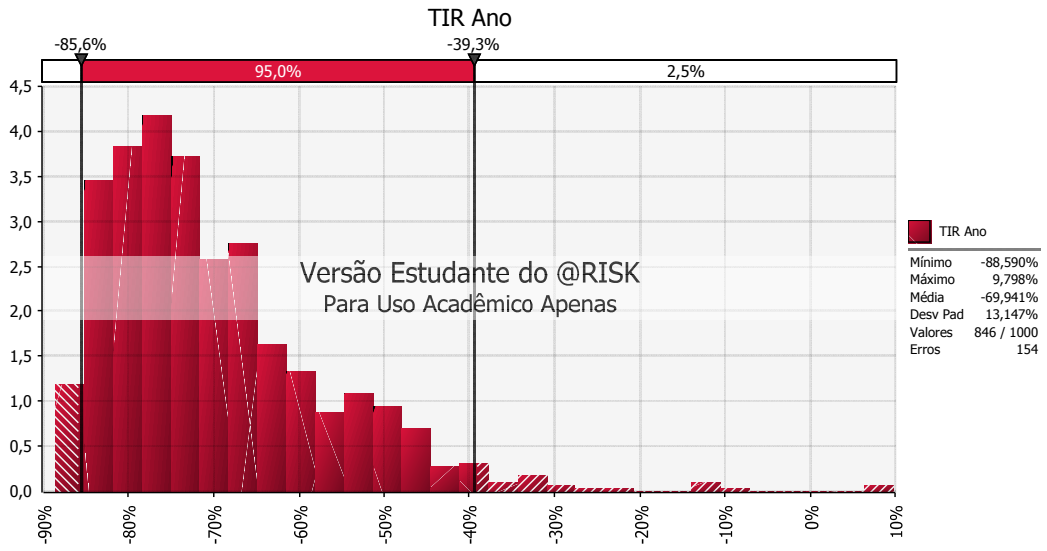


Figura 25: Probabilidade TIR com 95% de confiança- Cenário 3
Fonte: Elaboração própria

Na figura 26 verificam-se as variáveis que produziram maior influência nos resultados da simulação. Isto posto, além do efeito supracitado para o preço do Bitcoin e nível de dificuldade, fica evidenciado a importância da venda do ativo para o resultado, demostrando que a operação não obteve retorno financeiro meramente com a atividade de mineração.

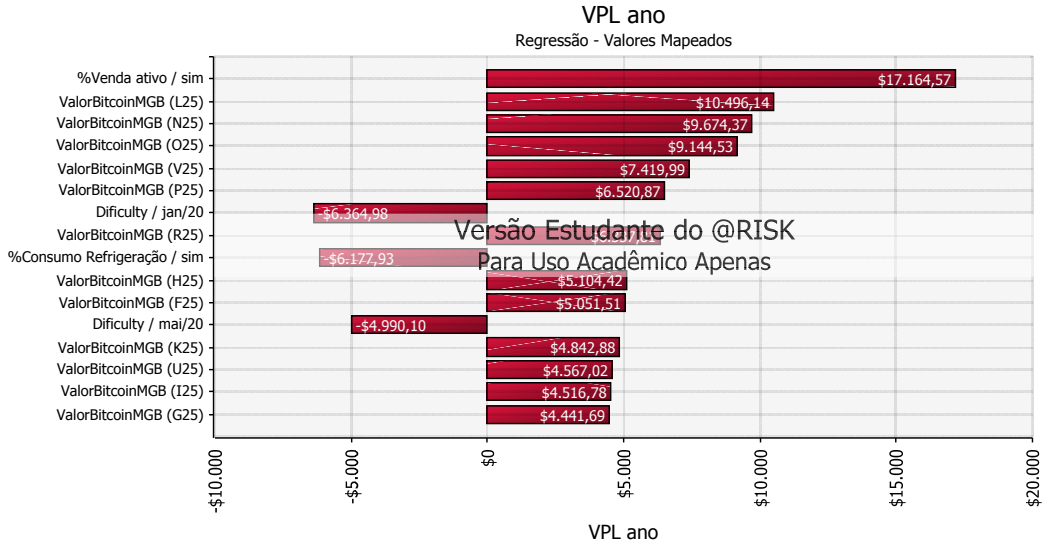


Figura 26: Graf. Tornado Sensibilidade VPL- Cenário 3
Fonte: Elaboração própria

Nas figuras 26, 28 e 29 são apontadas as correlações das variáveis de maior influência no modelo, com o resultado do VPL. Observa-se que a dado resultado do Bitcoin em 0,85, para a correlação de Pearson, expressa forte correlação do preço com o retorno financeiro do investimento. As demais variáveis, por possuírem uma correlação abaixo de 0,3, são consideradas desprezíveis.

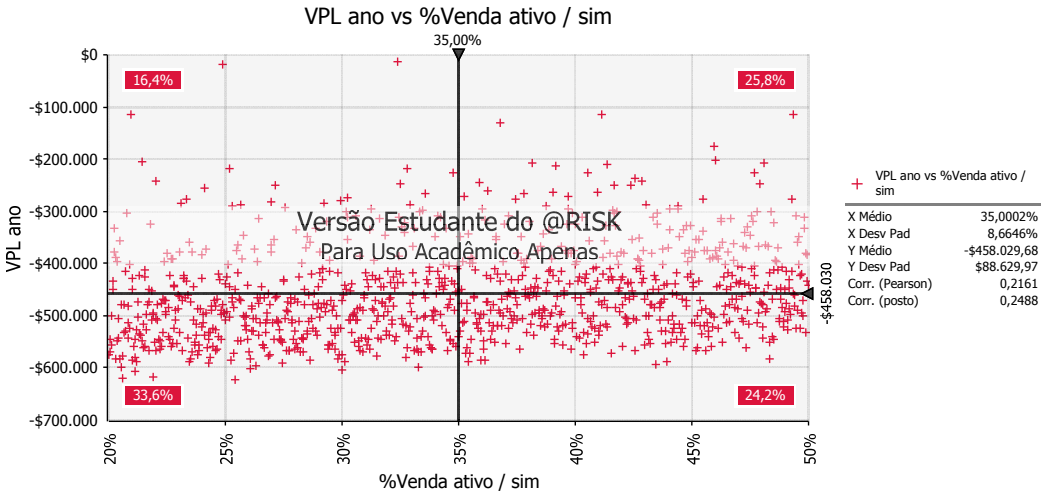


Figura 27: Correlação VPL versus Venda ativo- Cenário 3
Fonte: Elaboração própria

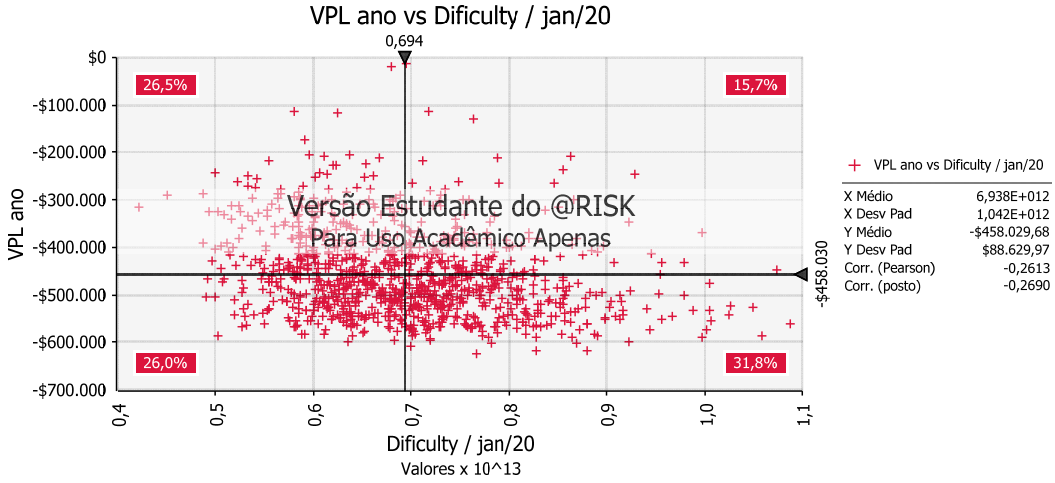


Figura 28: Correlação VPL versus Dificulty - Cenário 3
Fonte: Elaboração própria

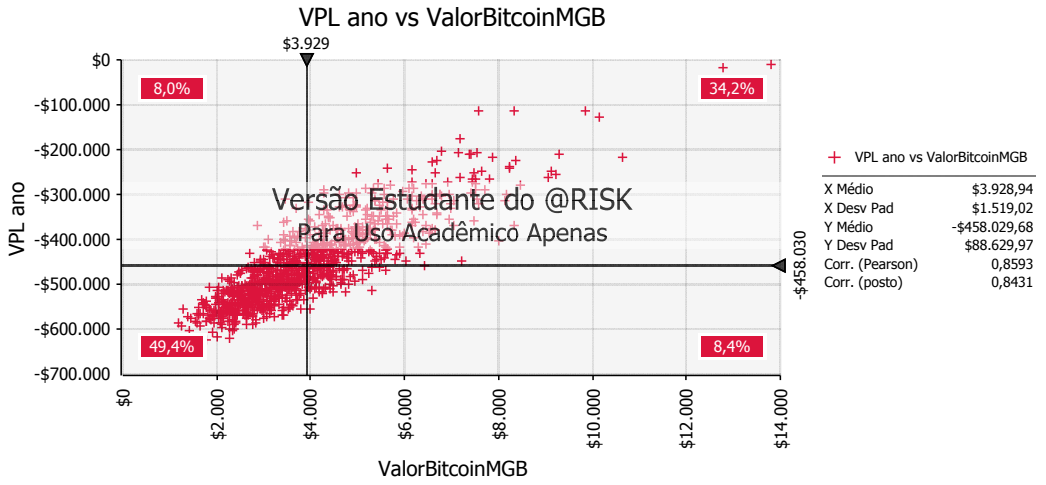


Figura 29: Correlação VPL versus Valor Bitcoin - Cenário 3
Fonte: Elaboração própria

Na figura 30 observa-se o orçamento acumulado em função do tempo do investimento, que evidencia que a operação ocorre em negativo, com maior declínio a partir do mês de maio de 2020, quando ocorre a redução da recompensa paga aos mineradores e maior amplitude de possibilidade de perdas em função do nível de dificuldade da rede. Por fim, fica demonstrado efeito positivo da venda dos equipamentos no mês de dezembro de 2020, embora seja irrelevante para reverter o resultado negativo do investimento.

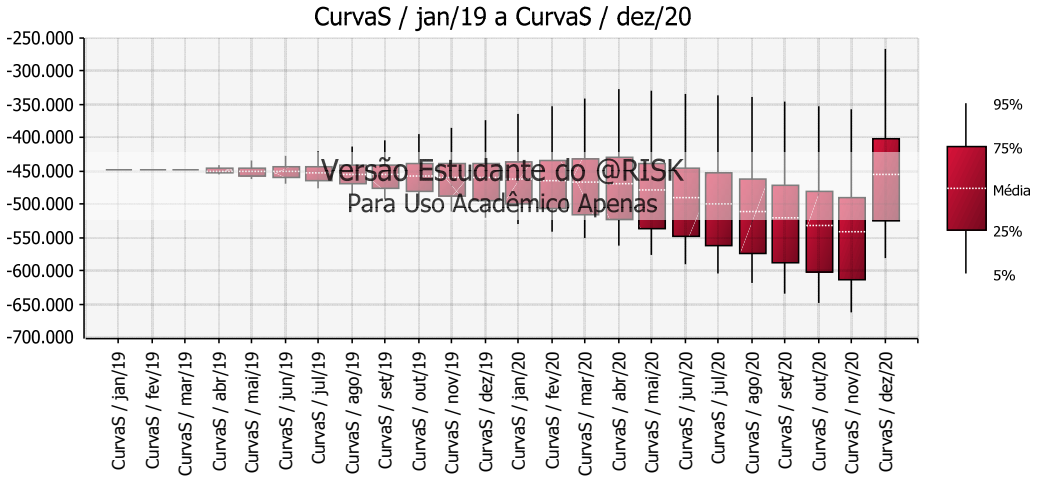


Figura 30: Curva S - Cenário 3
Fonte: Elaboração própria

Na figura 31 observa-se que fluxo de caixa do investimento opera em média próximo a zero, obtendo resultado positivo apenas no último mês, oriundo da venda dos equipamentos, conforme demonstrado na figura anterior. Por conseguinte, este é um indicativo que o investimento demandará um capital extra para manter a operação.

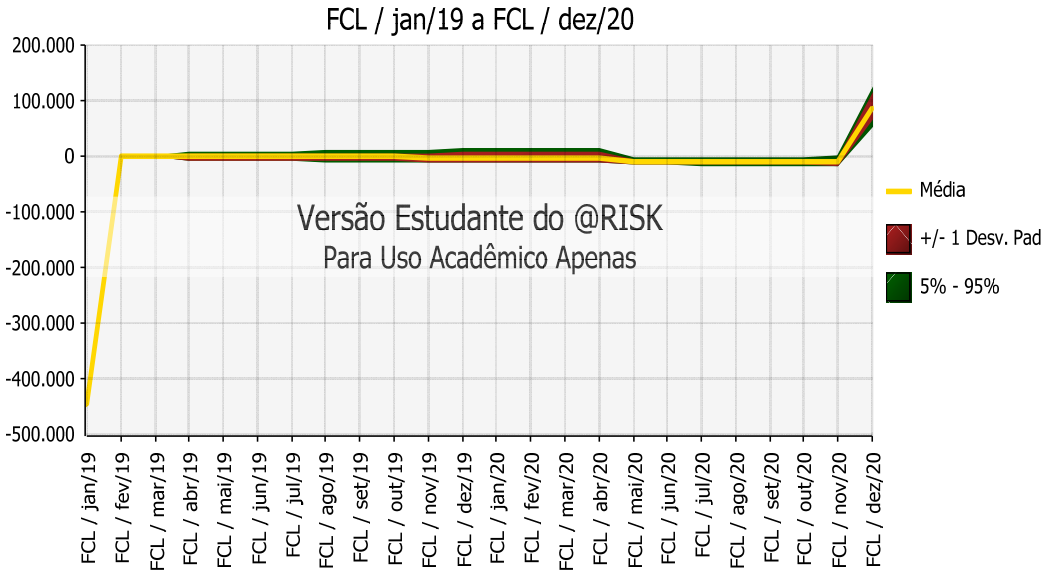


Figura 31: Fluxo de caixa - Cenário 3
Fonte: Elaboração própria

Nas figuras 32 e 33 são retratados os valores do Bitcoin e do nível de dificuldade obtidos durante as simulações. Nota-se que o valor estimado não é provável que o valor do Bitcoin atinja um valor superior a US$10.000 nos próximos 24 meses.

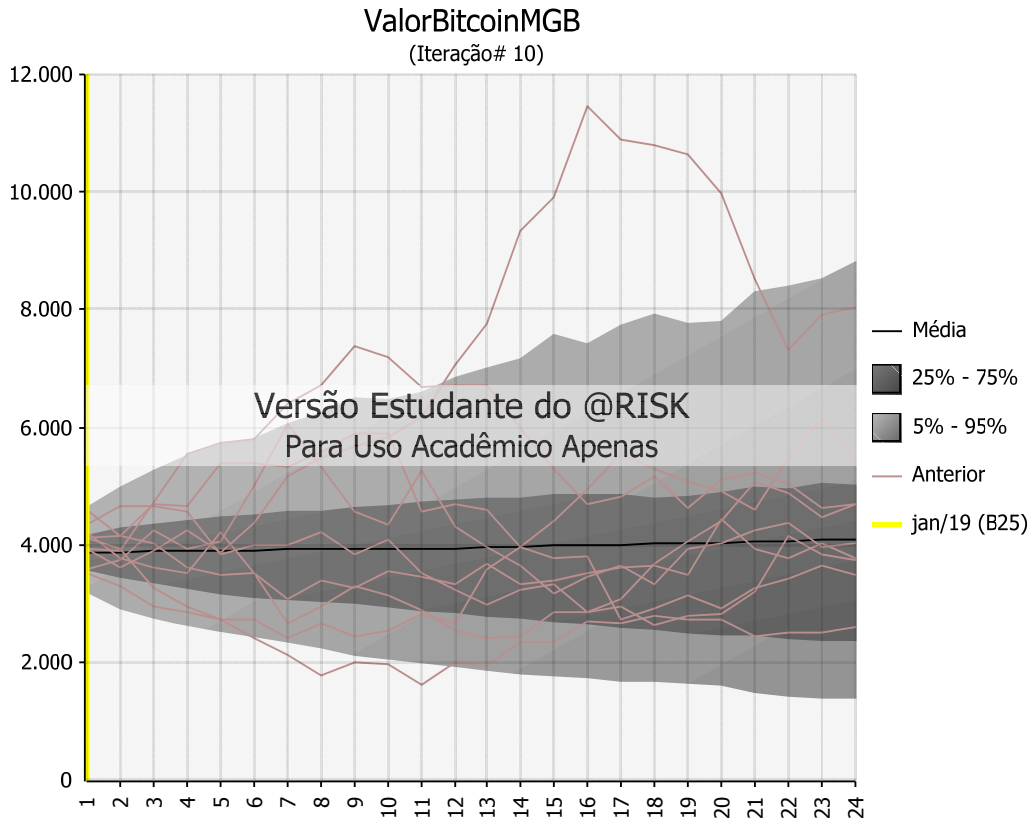


Figura 32: Simulação MGB para Bitcoin - Cenário 3
Fonte: Elaboração própria

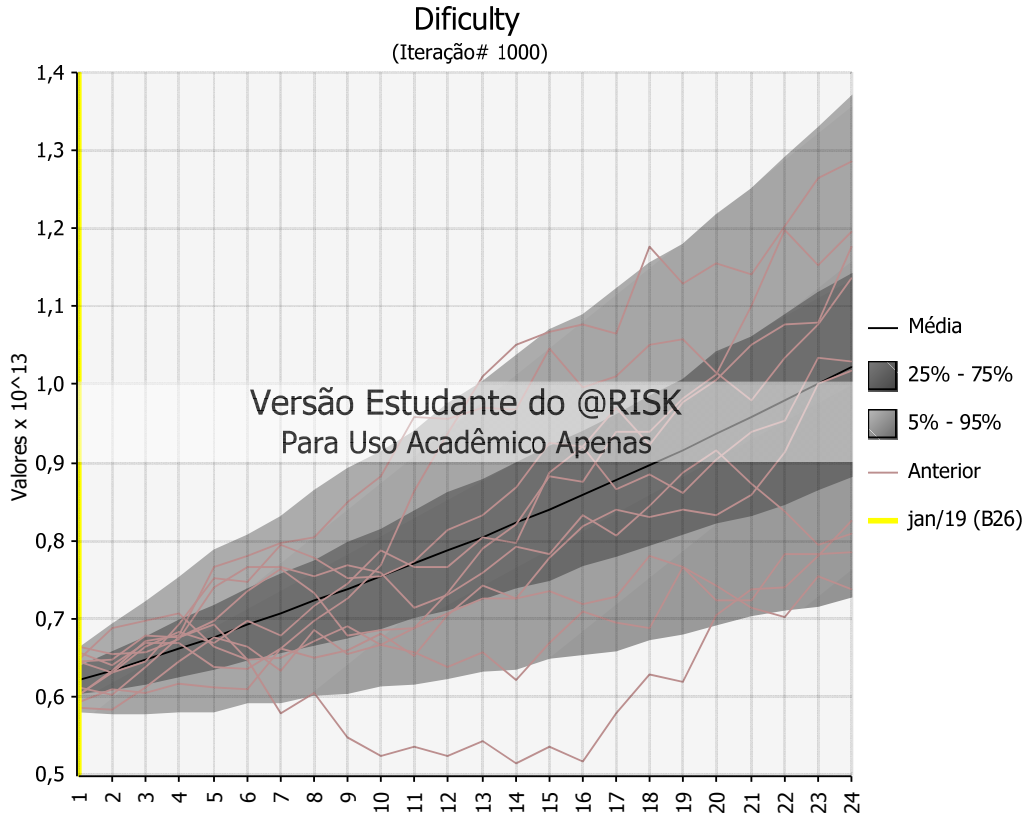


Figura 32: Simulação MGB para Dificulty - Cenário 3
Fonte: Elaboração própria.

5
Considerações finais

A indústria de mineração de criptomoedas ainda está passando por rápidas mudanças e transformações, frente ao seu ineditismo e principalmente em razão das incertezas quanto à sua consolidação no mercado.

Esse estudo estendeu o modelo proposto por Hayes (2015), se propondo a criar um fluxo de caixa descontado para analisar a rentabilidade econômica do investimento em mineração de Bitcoins. O foco dado foi para a operacionalização de uma fazenda de mineração no Brasil, com aquisição de até 100 mineradoras. Primeiramente foi desenvolvido um modelo determinístico, visando avaliar a viabilidade do investimento ao longo do tempo, em um cenário mais provável, um otimista e por fim um pessimista. Tendo em vista que os dois primeiros apresentaram resultados negativos, não foi analisado o pior cenário. Para aprofundar o entendimento dos resultados, foram efetuadas análises de sensibilidades, visando compreender as variáveis que mais afetam o modelo e suas relações com o resultado da taxa interna de retorno e valor presente líquido. Observou-se que a variável com maior correlação e, portanto, de maior sensibilidade no modelo foi o valor do Bitcoin. Considerando os parâmetros utilizados, só existe viabilidade de investimento no Brasil, com o Bitcoin cotado acima de US$ 10.000. Outra variável com grande influência no resultado foi o nível de dificuldade, que, quanto maior e mais acelerado, menor será a vida útil do equipamento e consequentemente menor será o retorno do investimento. O custo de energia também possui uma forte atuação no resultado, porém, conforme demonstrado na tabela 10, mesmo com custo zero, o resultado será negativo, em função do investimento para a atual cotação do Bitcoin. Este resultado apesar de inicialmente inconcebível, quando analisada na perspectiva da matemática financeira, é incontestável, tendo em vista o custo do investimento e o curto tempo de operação, que está pautado pela vida útil dos equipamentos. Desta forma, o custo do investimento passa a ter um peso relevante no retorno financeiro. Neste sentido, a taxa sobre importação também apresentará impacto no resultado, conforme demostrado na tabela 9. Tendo como objetivo obter uma visão mais holística dos riscos e aprimorar o processo de tomada de decisão, o modelo foi aperfeiçoado, com a inclusão de métodos

estocásticos, mas especificamente o Movimento Geométrico Browniano – MGB, para estimar no tempo o valor do Bitcoin e do nível de dificuldade, que são as variáveis com maior nível de incerteza do problema. Posteriormente foram efetuadas diversas simulações em diferentes cenários visando estimar o risco do investimento. No primeiro cenário foram considerados retorno e volatilidade histórica, que resultaram em 70% de probabilidade que o valor presente líquido seja abaixo de zero e ínfima possibilidade de obter uma TIR acima 2.500%. Esta amplitude é acarretada pela alta volatilidade das variáveis de incerteza. Desta forma, buscando efetuar um corte do período embrionário da criptomoeda, foi analisado o retorno para risco e volatilidade desde 2013. Este cenário resultou em 77,2% de probabilidade da TIR ser negativa e reduziu a magnitude dos elevados retornos. Por fim, foi analisada a probabilidade, levando em consideração o risco e volatilidade do último trimestre, que reduziu para nula a chance de sucesso do investimento e corroborou com os resultados anteriores, indicando a inviabilidade de investimento.

Acima de tudo é fundamental ressaltar que o alto investimento e a incerteza do valor do Bitcoin são fatores de risco limitadores para o investimento em mineração. Outrossim existem inúmeras outras incertezas, não contempladas no modelo, que podem acarretar prejuízo, as quais destacam-se, mas não se limitam ao bloqueio de mineração em ASIC, como ocorreu com a criptomoeda Monero em 2018; A mudança do protocolo de consenso de prova de trabalho(PoW) para prova de participação(PoS),como prevista para ocorrer no lançamento da versão Constantinopla do Etherium, segunda principal criptomoeda do mundo; Ao surgimento dos computadores quânticos, que podem colocar em risco todo mecanismo de criptografia atual da Blockchain e por último e não menos importante, as regulamentações em relação ao uso da criptomoeda e/ou ao mercado de mineração.

Um aspecto que merece destaque é que apesar do alto investimento para aquisição dos equipamentos, o custo mais expressivo no processo de mineração continua sendo o de eletricidade, em razão do gasto colossal de energia, necessário para garantir a prova de trabalho, exigida pelo Bitcoin. Isto posto, é notório que o custo de mineração irá depender primordialmente do custo de eletricidade. Nesta perspectiva e tendo em vista que a indústria de criptomoedas é geograficamente independente, observa-se maior vantagem em implantar as fazendas de minerações em países que proporcionam menor custo de eletricidade, que possuem clima com baixa temperatura, acesso rápido e estável à internet e menores taxas e regulamentações do governo. Esses fatores

evidenciam que o Brasil é um país desfavorável para esse tipo de atividade e explicam a concentração de mineradores em locais como a China.

Outra vertente que merece importância é o fato que o lucro das mineradoras está cada vez mais baixo, em virtude da redução da recompensa e da rápida taxa de obsolescência do hardware de mineração, impulsionada pelo quase ininterrupto incremento do nível de dificuldade. Isso acarreta em uma necessidade de melhor eficiência operacional e investimento contínuo em equipamentos. Essa conjuntura explica a mudança drástica do anterior cenário de descentralização para a centralização da operação, com o surgimento de grandes centros de mineração e integração vertical efetuada por algumas das fabricantes de equipamentos. Não obstante, estamos em um momento de inflexão do retorno do investimento em mineração, ocasionada pela relação do custo operacional e do valor de mercado do Bitcoin. Isso tem provocado o encerramento de diversas fazendas de mineração ao redor do mundo e a redução recente do nível de dificuldade. Pois, dependendo do cenário, não é rentável o investimento em mineração de Bitcoins, mesmo com baixo custo de energia. Neste caso, acaba sendo mais vantajoso atuar no trade de criptomoedas que na mineração das mesmas.

Ainda em linha com o modelo proposto, cabem discussões para estudos futuros sobre a operação em outros países, a viabilidade de mineração de outras criptomoedas, que possuem menor nível de dificuldade, menor necessidade de investimento e maior grau de alavancagem; Estudos relacionados à utilização de fontes alternativas de energia no processo de mineração. Outro aspecto que merece destaque e pode ser desenvolvido futuramente é o impacto ambiental do custo energético com a atividade de mineração e a relação entre os sistemas financeiros centralizados versus descentralizados

6
Referências bibliográficas

BADEV, A.; CHEN, M. **Bitcoin: technical background and data analysis**. 2014.

CEZAR, G. S. *et al*. **Fluxo De Caixa Projetado Considerando Os Efeitos Do Risco, Por Meio Da Simulação De Monte Carlo: Aplicado a Empresa De Pequeno Porte Do Setor De Comércio De Produtos Agropecuários**. [s. l.], 2018.

CHÁVEZ, J. J. G.; RODRIGUES, C. K. S. **Hopping among pools in the Bitcoin mining network**. Th e SIJ Transactions on Computer Networks & Communication Engineering (CNCE), v. 3, n. 2, 2015.

CHOW, S.; PECK, M. E. **The bitcoin mines of China**. IEEE Spectrum, [s. l.], v. 54, n. 10, p. 46–53, 2017.

CHUN, R. **Bitcoin Mining**. Atlantic, [s. l.], v. 320, n. 2, p. 26, 2017.

COSTA, L. G. T. A.; COSTA, L. R. T. A.; ALVIM, M. A. ***Valuation*: manual de avaliação e reestruturação econômica de empresas**. São Paulo: Atlas. 2010.

CUSUMANO, M. A. **The Bitcoin Ecosystem**. Communications of the ACM, [s. l.], v. 57, n. 10, p. 22–24, 2014.

DİLEK, Ş.; FURUNCU, Y. Bitcoin Mining and Its Environmental Effects. Ataturk University **Journal of Economics & Administrative Sciences**, [s. l.], v. 33, n. 1, p. 91-105, 2019.

DIXIT, A. K.; PINDYCK, R. S. **Investment under uncertainty**. Princeton University Press Princeton, NJ. 1994.

DOWD, K.; HUTCHINSON. M. Bitcoin will bite the dust. **Cato Journal**, v. 35, n. 2. 2015.

DU, X.; LI, A. N. **Monte Carlo simulation and a value-at-risk of concessionary project**: The case study of the Guangshen Freeway in China. Management Research News [S.I.], v. 31, n. 12, p. 912-921, 2008.

FAN, J. P. H. Price uncertainty and vertical integration: an examination of petrochemical firms. **Journal of Corporate Finance** [S.I.], v. 6, n. 4, p. 345-376, 2000.

GARVIN, M. J.; CHEAH, C. Y. J. **Valuation techniques for infrastructure investment decisions. Construction Management and Economics** [S.I.], v. 22, n. 4, p. 373-383, 2004.

GUIMARÃES, L. S. D.; SAMANÉZ, C. P. **Comparação entre o movimento geométrico browniano e processo de reversão à média com saltos para avaliação de opção de expansão para poços de petróleo**. [recurso eletrônico]. [s.l.] : 2002., 2002.

HAYES, A. **Cryptocurrency Value Formation**: An Empirical Analysis Leading to a Cost of Production Model for Valuing Bitcoin. [s. l.], 2015.

History of Bitcoin. Disponível em: <www.http://historyofbitcoin.org/>. Acesso em: 1 de outubro de 2018, 10:14:30

KOSIK, B. **Data centers used for bitcoin mining**: Data centers used for bitcoin mining have significant differences from their commercial data center counterparts. Consulting Specifying Engineer, [s. l.], n. 5, p. 20, 2018.

LUTHER, W. J. **Bitcoin and the future of digital payments**. 2015.

MOREIRA, R. A. Valuation: um estudo aplicado a uma empresa produtora de insumos siderúrgicos de Minas Gerais, 2015

NAKAMOTO, S. **Bitcoin: a peer-to-peer electronic cash system**. 2008.

NICOLAS HOUY. **The Bitcoin Mining Game. Ledger**, [s. l.], n. 0, p. 53, 2016.

NIELSEN, M. **How the Bitcoin protocol actually works**. 2013.

PADDOCK, J. L.; SIEGEL, D. R.; SMITH, J. L. Option Valuation of Claims on Real Assets: The Case of Offshore Petroleum Leases. **Quarterly Journal of Economics**, p. 479-508, August, 1988.

PERCIVAL, C. **Stronger key derivation via sequential memory-hard functions**. 2009.

POON, J.; THADDEUS, D. **The Bitcoin lightning network**: acalable off-chain instant payments. 2016.

ROSENFIELD, M. **Analysis of Bitcoin pooled mining reward systems**. 2011.

SILVA, R. I.; PINTO, C. L. B.; BRANDÃO, L. E. T. **Um modelo geral para tomada de decisão sob incerteza e flexibilidade em parcerias público-privadas**. [recurso eletrônico]. [s.l.] : 2016., 2016.

WHITE, L. H. The market for cryptocurrencies. **Cato Journal**. v. 35, n. 2, 2015.

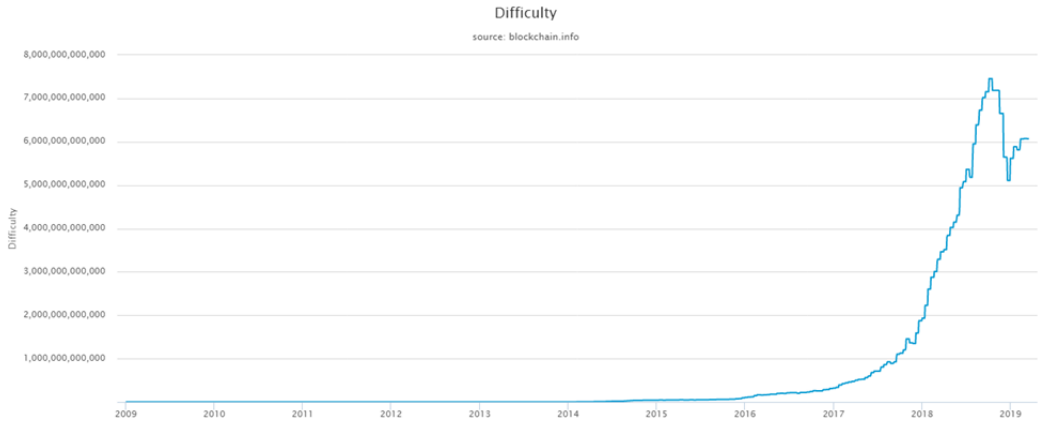
Anexo 1 - Gráficos da Blockchain Bitcoin

Visão Histórica do preço de mercado do Bitcoin

Visão 2013 à 2017 do preço de mercado do Bitcoin

Visão 2012 à 2014 do preço de mercado do Bitcoin

Nível de dificuldade da rede



Recompensa em mineração