UNIVERSIDADE FEDERAL DO CEARÁ
FACULDADE DE ECONOMIA, ADMINISTRAÇÃO, ATUÁRIAS, CONTABILIDADE E SECRETARIADO EXECUTIVO - FEAAC
CURSO DE CIÊNCIAS ECONÔMICAS

EDSON BRUNO RODRIGUES MOREIRA

GESTÃO DE PORTFÓLIO DE CRIPTOMOEDAS

FORTALEZA
2022

EDSON BRUNO RODRIGUES MOREIRA

GESTÃO DE PORTFÓLIO DE CRIPTOMOEDAS

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Ciências Econômicas do Departamento de Economia Aplicada da Universidade Federal do Ceará como requisito para a obtenção do Bacharel em Ciências Econômicas.

Orientador: Prof. Dr. Vitor Borges Monteiro

FORTALEZA

2022

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Sistema de Bibliotecas
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

M837g Moreira, Edson.
Gestão de portfólio de criptoativos / Edson Moreira. – 2022.
44 f. : il. color.

Trabalho de Conclusão de Curso (graduação) – Universidade Federal do Ceará, Faculdade de Economia, Administração, Atuária e Contabilidade, Curso de Ciências Econômicas, Fortaleza, 2022.
Orientação: Prof. Dr. Vitor Borges Monteiro.

1. Gestão de criptoativos. 2. Investimentos. 3. Criptografia. 4. Crise de 2008. I. Título.

CDD 330

EDSON BRUNO RODRIGUES MOREIRA

GESTÃO DE PORTFÓLIO DE CRIPTOMOEDAS

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Ciências Econômicas do Departamento de Economia Aplicada da Universidade Federal do Ceará como requisito para a obtenção do Bacharel em Ciências Econômicas.

Orientador: Prof. Dr. Vitor Borges Monteiro

Aprovada em: 05/12/2022.

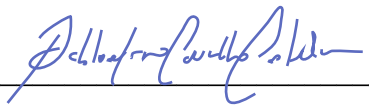
BANCA EXAMINADORA

Professor Dr. Vitor Borges Monteiro (Orientador)

Universidade Federal do Ceará – UFC (Membro)

Professor Dr. Wesley Leitão de Souza

Universidade Federal do Ceará – UFC (Membro)



Professor Dr. Pablo Urano de Carvalho Castelar

Universidade Federal do Ceará – UFC (Membro)

AGRADECIMENTOS

Agradeço em primeiro lugar a Ele, nosso Senhor, por possibilitar com o seu amor infinito que eu, uma mera criatura, pudesse existir com saúde e por meio de uma mulher que lutou desde sua adolescência para que eu pudesse chegar aqui. A esta mulher, Cinária Rodrigues, que carregou a mim em sua barriga por nove meses e cuidou-me por mais vinte e um anos, mesmo que para isso ela precisasse sacrificar muitas coisas.

Ao meu mais antigo amigo Josadak Neto, que me auxiliou no processo de conversão total ao catolicismo, ao Padre Paulo Ricardo que me ensinou muito sobre a beleza da igreja e aos incontáveis filósofos, economistas, empreendedores etc. Em destaque ao venerável mestre Olavo de Carvalho e a Roger Scruton, que Deus os tenha.

A minha amiga e queridíssima madrinha de bastismo e crisma, Amanda Maia e seu, assim espero, futuro marido, e agora meu padrinho de batismo, Paulo Davi Pessoa. A todos aqueles e aquelas que me ajudaram direta ou indiretamente a chegar aqui. A meus colegas Wisley Borges e José Airton por não me deixarem desistir do curso e a meu caro amigo Márcio (Piauí) Roberto por aturar-me desde o início do curso.

Por fim, vale fazer uma honraria ao meu orientador, Prof. Dr. Vitor Borges Monteiro por ter tido um incrível *insight* de ajudar-me a escolher um tema que fosse mais amplo, abrangendo uma carteira somente de criptoativos e para um período mais alongado, o que possibilitou resultados diferentes aos artigos comumente publicados sobre o tema. Também um agradecimento à banca (Wesley Leitão e Pablo Castelar) por ter disposto seu tempo para analisar o trabalho.

RESUMO

Este trabalho é resultado do estudo e análise das criptomoedas como forma de investimento, desde sua base teórica até sua aplicação prática. O objetivo principal foi analisar o resultado das carteiras criadas e sua comparação com o benchmark de Fundos de Investimento Multimercado (FIM). O mesmo foi dividido em três partes: primeiro, foi realizada uma pesquisa exploratória que visou descrever a base histórica e tecnológica dos criptoativos; segundo, pelo mesmo método de pesquisa, foi realizada a revisão de literatura sobre a Seleção de Carteiras de Markowitz; e terceiro, foi elaborado uma pesquisa descritiva e quantitativa, com um universo de 1034 observações diárias, no período de 01 de janeiro de 2020 a 31 de outubro de 2022 para sete ativos. Obteve-se como resultado que os criptoativos possuem correlação próxima, alta volatilidade e possuem correlação maior com o Bitcoin. Como conclusão, as carteiras encontradas (exceto uma delas) superaram o benchmark de FIMs.

Palavras-chave: Gestão de criptoativos. Investimentos. Criptografia. Crise de 2008.

ABSTRACT

This work is the result of the study and analysis of cryptocurrencies as a form of investment, from its theoretical basis to its practical application. The main objective was to analyze the result of the created portfolios and their comparison with the Multimarket Investment Trusts (MIT) benchmark. It was divided into three parts: first, an exploratory research was carried out that aimed to describe the historical and technological basis of crypto-assets; second, by the same research method, a literature review on Markowitz Portfolio Selection was carried out; and third, a descriptive and quantitative research was elaborated, with a universe of 1034 daily observations, in the period from January 1, 2020 to October 31, 2022 for seven assets. It was obtained as a result that cryptoassets have a close correlation, high volatility and have a greater correlation with Bitcoin. In conclusion, the portfolios found (except one of them) outperformed the MITs benchmark.

Palavras-chave: Crypto asset management. Investments. Cryptography. 2008 crisis.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

Após a Crise do subprime de 2008-09, a ideia de o dinheiro estar sob o controle unicamente de um Estado centralizado, servindo de intermediário financeiro, ganhou ainda mais notoriedade. Com os Bancos Centrais cada vez mais atuantes e modificando a estrutura econômica não só dos Estados Unidos, mas do mundo como um todo, veio a necessidade do surgimento de uma tecnologia que permitisse que o poder monetário ficasse nas mãos da população, do povo. E essa necessidade é válida mesmo para os países que adotaram um "pai dos bancos" autônomo, como foi o caso do Brasil em 2021, ou independente, caso dos Estados Unidos com o *Federal Reserve (FED).* Sendo, pelo mesmo critério, uma necessidade para os países que não possuem nenhum dos casos ditos, visto que estes podem intervir na economia por motivos políticos, gerando casos de instabilidade monetária, como a hiperinflação. E para os primeiros casos, com o seu processo de ajuste inflacionário e de juros (políticas de expansão ou retração monetária) os mesmos acabam por, ao longo do tempo, reduzir o valor real da moeda nacional. Por esse motivo, Satoshi Nakamoto afirma,

> O comércio na Internet tem dependido quase exclusivamente de instituições financeiras que servem como terceiros confiáveis para processar pagamentos eletrônicos. Enquanto o sistema funciona bem para a maioria das operações, ainda sofre com as deficiências inerentes ao modelo baseado em confiança. [...] O que é necessário é um sistema de pagamento eletrônico baseado em prova criptográfica em vez de confiança, permitindo a quaisquer duas partes dispostas a transacionar diretamente uma com a outra sem a necessidade de um terceiro confiável (NAKAMOTO; 2008, p. 1).

A citação acima é um resumo da história das criptomoedas e da criptografia, visto que, depois do fim da paridade com o ouro em 1971 nos Estados Unidos, as moedas (o dólar, em específico) passaram a ter o seu lastro econômico baseado puramente na confiança que a população possui para com o Governo e sua economia. Dessa forma, caso o Governo (ou o Banco Central autônomo ou independente) faça uma intervenção na base monetária, como uma expansão monetária que venha a causar uma hiperinflação, o que o impediria seria a revolta popular, a impopularidade e a perda de confiança. A exemplo, têm-se o caso da Venezuela, que em 2018 registrou 130.060% de inflação (ARRAEZ; VALDERRAMA, 2022).

Porém, a pauta da liberdade monetária é defendida há décadas por liberais como Friedrich Hayek, libertários como Murray Rothbard, criptoanarquistas como Timothy C. May e cypherpunks como Eric Hughes. Segundo Rothbard (2010), mesmo que em uma situação

hipotética em que o governo intervenha somente para o bem estar populacional, a incerteza por ser um sistema centralizado, que não permita competição, faz o sistema como um todo ser ineficiente e inseguro. Necessitando de alguma solução que possibilite que a população não fique à mercê do Estado, que possa se proteger da incerteza e da ineficiência.

Para isso, muitos nomes surgiram com ideias disruptivas, sugerindo métodos de pagamento e troca sem que houvesse a necessidade de um intermediário financeiro ou que tal intermediário fosse limitado. Foram os casos do eCash de David Chaum, CyberCash de Daniel C. Lynch e outros, E-Gold do Dr. Douglas Jackson e Barry Downey, Hashcash do Adam Back, BitGold de Nick Szabo e b-money de Wei Dai. Em cada caso, a tecnologia foi evoluindo e tornando-se cada vez mais independente de terceiros, e anônima, até culminar com o surgimento do *whitepaper* do Bitcoin, por Satoshi Nakamoto, em 31 de outubro de 2008, com a proposta de ser um sistema monetário sem intermediários, sendo protegido por uma rede *peer-to-peer* por meio da Blockchain (NAKAMOTO; SATOSHI, 2008). Porém, até o surgimento do Bitcoin ocorreu um avanço criptográfico e matemático sem precedentes, saindo de um sistema TCP/IP (anterior à própria internet), para o surgimento de uma comunicação de dados totalmente anônima, e sem intermediários.

Após o surgimento do Bitcoin, uma imensidade de projetos monetários e contratuais, *smart contracts*, foram desenvolvidos por comunidades de desenvolvedores. E cada projeto deste possui (ou deveria possuir) um fundamento que faz os investidores terem uma esperança de que no futuro estes tenham uma maior utilização no dia a dia e retornem lucros extraordinários. Dessa forma, precisa-se descobrir a plausabilidade de criptoativos como forma de investimento e se a adesão de uma carteira composta totalmente pelos mesmos é rentável. Vale destacar que Silva e Monteiro (2021) estudaram o perfil dos usuários de criptomoedas no Brasil, bem como o comportamento da criptoeconomia e o processo regulatório, e concluíram que as características das criptos assemelham-se mais a ativos do que a moedas.

Segundo o Google, sua retrospectiva anual de 2021 teve como um termo de busca em destaque o “Como comprar bitcoin”, chegando a superar a expressão “Como comprar ações”. Demonstrando que cada vez mais investidores estão dispostos a se arriscarem nesse novo investimento, seja visando ganhos imediatos ou de longo prazo. Além disso, tem-se a adesão desta criptomoeda no meio das celebridades, sendo Elon Musk, Personalidade do Ano de 2021 pela revista Time, um adepto que influenciou os mercados, divulgando a moeda em suas redes sociais e permitindo a compra de seus carros em uma de suas empresas, a Tesla Motors (CORACCINI; RAPHAEL, 2021) (BALL; MOLLY, 2021).

Em meio a este cenário, é preciso descobrir se uma carteira de criptoativos é plausível a ser adotada como forma de investimento. Aja vista que a variação dos preços dos mesmos, em geral, é exponencial. Para efeito de comparação, o Bitcoin, a criptomoeda mais conhecida no mercado, saltou em 1 de janeiro de 2021 de aproximadamente U$29.000 para U$67.000 em 10 de novembro de 2021, ou seja, mais de 135% de valorização em menos de um ano. E ao mesmo tempo, desde o dia 11 de novembro de 2021, ocorre uma queda de preços de mais de 70% (TOLOTTI, RODRIGO, 2021) E no mesmo período, a criptomoeda Polygon (MATIC), valorizou mais de 12.000%, com queda posterior de 50%. Ou seja, a variação de preços entre os criptoativos é distinta.

Os fatos apresentados fazem alguns investidores fundamentalistas e renomados, como Charlie Munger e Warren Buffet, vice-presidente e presidente da Berkshire Hathaway respectivamente, a se oporem às moedas digitais, fazendo críticas a como elas funcionam e as chamando de “repugnantes e contrárias aos interesses da civilização” (LI; YUN, 2021).

O objetivo geral da pesquisa é responder à pergunta: quais os resultados provenientes da gestão de uma carteira de criptoativos para o investidor? E em específico: qual a correlação, covariância, volatilidades (riscos), retornos e desvios-padrão das carteiras estudadas. Resultados estes provenientes da maximização do retorno, da minimização da variância e da maximização da relação risco-retorno. Por fim, será feio um comparativo dos resultados obtidos com o benchmark de fundos multimercado para o mesmo ano.

Quanto à estruturação do trabalho, o mesmo é dividido em sete partes: (i) introdução, informando os motivos da criação do trabalho; (ii) revisão de literatura, para apresentar a base histórica e criptográfica dos criptoativos; (iii) diversificação, onde ocorrerá a apresentação da base financeira que possibilitará encontrar os dados para a formação das carteiras alvos do estudo; (iv) metodologia, demonstrando de que maneira e recursos serão utilizados para a produção do trabalho; (v) resultados, apresentando o que fora descoberto; (vi) conclusão, a qual será explicado o que foi utilizado no projeto e ideias para novos estudos futuros; (vii) referências, base histórica e informacional utilizada.

2 REVISÃO DE LITERATURA

2.1 CRIPTOMOEDAS

Após a expansão midiática causada pelo aumento do preço do Bitcoin, principal criptomoeda em valor de mercado, em 2013 (de US$ 21,00 para US$ 1.120), 2017 (de US$

1.000 para US$ 20.000) e 2021 (de US$ 29.446 para US$ 69.700) as moedas digitais passaram a ser alvo de curiosos em busca de enriquecimento rápido[1]. Entretanto, com a expansão da tecnologia e formação de uma ampla comunidade de pessoas dedicadas a criar projetos, as mesmas passaram a ser utilizados amplamente como forma de investimento e especulação, formação de contratos digitais, base monetária em jogos, autenticação de obras de arte digitais, transações de diversos valores, banco de dados, segurança de casas e empresas etc.

Mas antes da criação do Bitcoin, que será apresentado com destaque logo a frente, o surgimento de uma moeda totalmente digital passou por um processo de criação longo e complexo. Sendo necessário conhecer diversos campos de estudo para poder compreender o que fundamenta tais moedas, pois as mesmas foram um resultado de trabalho de programadores, criptógrafos, economistas e filósofos. E por este mesmo motivo, de ser totalmente digital, é alvo de críticas de uma mesma gama de pessoas de ilibada reputação, tal como o maior investidor ainda vivo, Warren Buffet. Visto isso, faz-se mister apresentar os fundamentos que vieram a dar base ao Bitcoin e posteriores moedas digitais.

2.2 A BASE CRIPTOGRÁFICA

O surgimento das criptomoedas, assim como o de uma infinidade de outras tecnologias criptográficas da contemporaneidade, só foram possíveis com o desenvolvimento do protocolo TCP/IP, do qual a internet faz uso. Em 1974, Vinton Gray Cerf e Robert Kahn, ambos ganhadores do Prêmio Turing, um importante prêmio para descobertas dentro da ciência da computação, publicaram o artigo *A Protocol for Packet Network Intercommunication* (um protocolo para intercomunicação de rede de pacotes, tradução livre). O artigo demonstrava como funcionaria a comunicação entre *HOSTS*, ou seja, entre indivíduos dentro de um ambiente compartilhado, como uma ponte (*bridge*) que ligaria dados dos indivíduos a uma rede (CERF; KAHN, 1974). Dessa forma, uma importante base das criptomoedas foi criada: a comunicação direta de um ponto a outro sem a necessidade de um servidor ou autoridade central.

O segundo protocolo fundamental que garante segurança superior à comunicação de um indivíduo a outro foi desenvolvido pelos matemáticos e criptógrafos Whitfield Diffie e Martin Hellman. Em 1976, por meio do artigo *New Directions in Cryptography* (novas direções em criptografia, tradução livre), Diffie e Hellman demonstraram como funcionaria a

[1] Como o caso de pirâmides financeiras, a exemplo a do "Faraó dos Bitcoins", investigado pela Polícia Federal (PF). Para maiores detalhes do caso, olhar página 17.

comunicação entre indivíduos por meio de uma chave pública (*public-key*) e uma chave privada (*private-key*). A primeira poderia ser criada por qualquer indivíduo, podendo ser disseminada a qualquer outra pessoa, visto que a mesma estaria criptografada, sem permitir que ninguém fizesse sua leitura. E a segunda deveria ficar guardada em segurança por parte do destinatário, pois a mesma é que permite a leitura dos dados criptografados (DIFFIE; HELLMAN, 1976). E isso é possível, pois, para romper uma chave pública, é necessário um consumo computacional em resolução de problemas matemáticos que atualmente não permitem uma solução eficiente, e são inerentes a determinadas relações de fatoração inteira, logaritmo discreto e curva elíptica.

Diffie e Hellman (1976) propuseram quatro axiomas que um sistema de chave pública deveria satisfazer, porém, foi somente com os matemáticos Ron Rivest, Adi Shamir e Leonard Adleman (RSA) em 1978, por meio do artigo *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems* (um método para obter assinaturas digitais e criptossistemas de chave pública, tradução livre) que foi possível descobrir as funções matemáticas que satisfaziam essas quatro regras. Esse método funciona desta maneira: de forma matemática, é feito a criptografia de uma mensagem, representado a mesma com o número *M*. Esse número é elevado a uma potência *e* que é publicamente conhecida. O número que resulta é dividido por outro número de conhecimento público, *n.* Porém, e aqui que está a parte importante do modelo, *n* é um produto de dois grandes números primos secretos *p* e *q*, assim, a segurança do sistema é dependente da dificuldade em fatorar *n* em *p* e *q* (SIDHU, 2021).

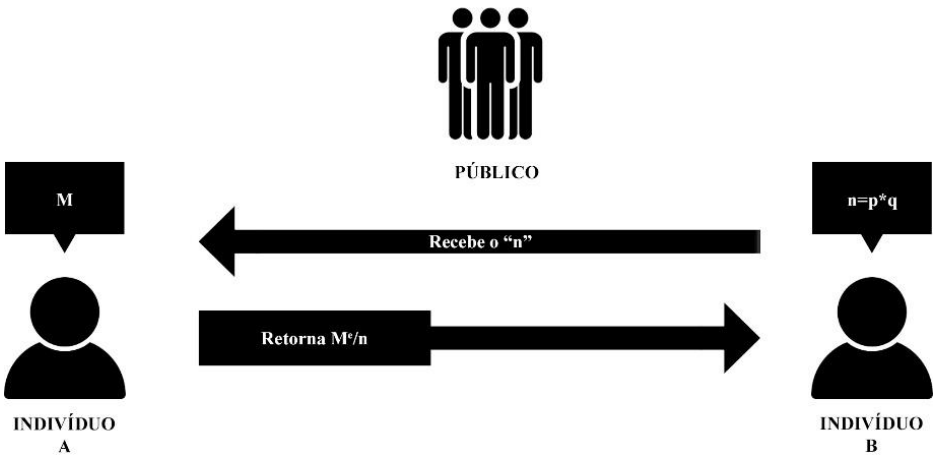


FIG. 1: Processo de envio de dados entre indivíduos. Elaboração própria.

Outra contribuição importante à estrutura criptográfica às criptomoedas foi elaborada por Ralph Merkle em 1979, com o conceito patenteado de árvores de *hash* (Figura

2). Em 1987 publicou o artigo *A Digital Signature Based on a Conventional Encryption Function* (uma assinatura digital baseada em uma função de criptografia convencional, tradução livre), com o qual solucionou dois problemas criptográficos de envio de informações de um ponto ao outro. Mas para entender isso é preciso primeiro explicar o conceito da função *hash*. A função *hash* recebe dados e faz a transformação dos mesmos em um número hexadecimal de tamanho fixo, este, chamado *hash*. Assim, se houver a alteração de um único bit dos dados o *hash* resultante será totalmente alterado. Garantindo com isso a autenticidade no bloco de dados (MERKLE, 1979).

Entretanto, para efetuar a garantia da integridade dos dados, é preciso fazer o envio de seu *hash* junto com os dados. Assim, o destinatário poderá calcular o *hash* dos dados e fazer sua combinação com o *hash* que foi enviado junto com os dados. Aqui surgem os dois problemas: o primeiro é que se alguém fizer a adulteração dos dados ao longo do caminho, este também poderia alterar o *hash*; segundo, se alterarem somente os dados, haverá a detecção da alteração, porém será preciso reiniciar o *download*, acarretando em sobrecarga da rede (SIDHU, 2021). Com a árvore de Merkle soluciona-se os dois problemas, pois os dados passam a ser divididos em pedaços e calcula-se um *hash* para cada pedaço. Após isso organiza-se todos os *hashes* como nós folhas de uma árvore e segue-se calculando em cada camada. E com a internet, os pedaços são distribuídos, e toda tentativa de adulterar um *hash* é preciso adulterar todos os diferentes pedaços de dados, modificando individualmente seus *hashes*. Com isso, faz o sistema ser distribuído e menor em tamanho, visto que reduz a quantidade de pedaços caso seja necessário reiniciar todo o sistema (MERKLE, 1979) (KANSAL, 2020).

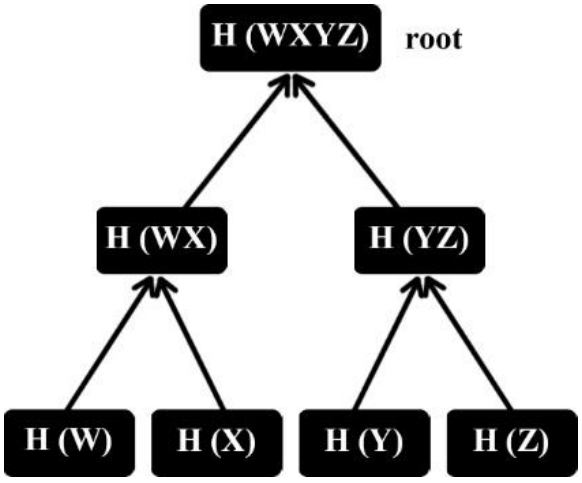


FIG. 2: Árvore de Hash. Elaboração própria

Com a evolução da criptografia RSA e das árvores de Merkle, o criptógrafo David Chaum publica em 1983 o artigo *Blind Signatures for Untraceable Payments* (assinaturas cegas para pagamentos não rastreáveis, tradução livre). O mesmo veio a trazer um problema: "considere o problema enfrentado por um administrador que deseja realizar uma eleição por voto secreto, mas os eleitores não conseguem se reunir para colocar seus votos em um único chapéu. Cada eleitor está muito preocupado em manter seu voto em segredo do administrador, e cada eleitor também exige a capacidade de verificar se seu voto foi contado" (Tradução livre do artigo original) (CHAUM, 1983, p. 200). E como solução, o autor afirma: "uma solução pode ser obtida usando os envelopes especiais. Cada eleitor coloca um boletim de voto com seu voto escrito nele em um envelope forrado de carbono; coloca o envelope revestido de carbono em um envelope externo endereçado ao administrador, com seu próprio endereço de retorno; e envia os envelopes aninhados para o administrador. Quando o administrador recebe um envelope externo com o endereço de retorno de um eleitor nele, o administrador remove o envelope interno forrado de carbono do envelope externo; assina a parte externa do envelope revestido de carbono; e envia o envelope revestido de carbono de volta, em um novo envelope externo, para o endereço do remetente no envelope externo antigo. Assim, apenas os eleitores autorizados recebem boletins de voto assinados. Claro, o administrador usa uma assinatura especial que só é válida para a eleição!" (Tradução livre) (CHAUM, 1983, p. 200).

Chaum ainda desce críticas ao modelo bancário de sua época, que ainda não mudou muito ao que se tem na atualidade, afirmando que o conhecimento de onde e como é feito o gasto do dinheiro pelo indivíduo revela informações que são privadas dele, violando com isso sua privacidade. E os sistemas de pagamentos anônimos, tal como o dinheiro, são privados, porém incorrem de serem mal utilizados e de sofrerem com a falta de segurança. Assim, o criptógrafo começou a definir o modelo de uma criptomoeda, a partir de três propriedades: (i) incapacidade de terceiros para determinar o beneficiário, o tempo ou o valor dos pagamentos feitos por um indivíduo; (ii) capacidade dos indivíduos de fornecer prova de pagamento ou de determinar a identidade do beneficiário em circunstâncias excepcionais; e (iii) capacidade de interromper o uso de meios de pagamento relatados como roubados (CHAUM, 1983).

Chaum também publica em 1981 o artigo *Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms* (Correio eletrônico não rastreável, endereços de retorno e pseudônimos digitais, Tradução livre), a qual promove o uso de pseudônimos de forma a proteger a identidade das partes comunicantes, e ao mesmo tempo, permite que ambos verifiquem a autenticidade. Introduzindo assim o conceito de um sistema de e-mail que permite

que as partes se comuniquem por endereços de e-mail não rastreáveis. A tecnologia subjacente desta foi denominada de *Mix Networks* (CHAUM, 1984).

Outras duas questões essenciais à criptografia foram o desenvolvimento da Criptografia de Curva Elíptica e a Impossibilidade de FLP. A primeira foi desenvolvida pelo Dr. Neal Koblitz e o Dr. Victor Miller em 1985, garantindo maior segurança ao sistema RSA, visto a impossibilidade computacional de resolver operações com logaritmo discreto de um elemento de curva elíptica (SIDHU, 2021). A segunda foi demonstrada por Michael Fischer, Nancy Lynch e Michael Paterson (FLP) no artigo *Impossibility of Distributed Consensus with One Faulty Process* em 1985. Neste, os autores provaram a impossibilidade de se conseguir um consenso em um sistema assíncrono (FISHER; LYNCH; PATERSON, 1985).

Há o nascimento da internet em 1990 e a criação de mais um protocolo que viria a ser mencionado no *whitepaper* do Bitcoin por meio dos artigos, estes são: *How to Time-Stamp a Digital Document* (como marcar a data e hora de um documento digital, tradução livre) divulgado pelos criptógrafos Stuart Haber e W. Scott Stornetta em 1991 e *Improving the Efficiency and Reliability of Digital Time-Stamping* (melhorando a eficiência e a confiabilidade da marcação de tempo digital, tradução livre), também elaborados por Stuart Haber e W. Scott Stornett, com a participação do matemático Dave Bayer em 1992. Estes artigos viriam a demonstrar como iria ser desenvolvido a marcação temporal dos blocos de *HASH*, criando a ideia de uma cadeia de *hashs* que cresce de maneira dinâmica utilizando as árvores de Merkle. Assim, cria-se um sistema composto por usuários, um Time-Stamp Service (TSS) e um repositório de dados, a qual a partir de um intervalo regular a TSS publica um “hash de intervalo” em um repositório que é disponível amplamente, criando uma sequência de etapas que permitem validar o carimbo data/hora de um documento (SIDHU, 2021).

Em 1991 há também a invenção de Phil Zimmermann do *Pretty Good Privacy* (PGP), uma forma de assinar, criptografar e descriptografar mensagens, e-mails e arquivos por meio de caracteres aleatórios que tornam praticamente impossível ataques de hackers (SIDHU, 2021).

2.3 PRIMEIRAS CRIPTOMOEDAS

Os primeiros relatos de indivíduos criando projetos visando uma moeda totalmente digital e que não necessitasse de um terceiro mediador, como o Banco Central, remonta desde o século passado, com a criação do eCash pelo criptógrafo David Chaum em 1983. Ele conceituou uma moeda simbólica que conseguia fazer a transferência entre indivíduos, de

maneira privada e segura, por meio do já mencionado sistema *blind signature* (assinatura cega, em português). Após a criação do eCash, Chaum criou a empresa DigiCash em 1989, de forma a colocar em prática todo os conceitos de criptografia criados até o momento. Entretanto, como a empresa decretou falência em 1998, esta serviu de base para outros projetos futuros (REIFF, 2022).

Em 1994, Daniel C. Lynch, William N. Melton, Steve Crocker e Bruce G. Wilson fundaram a CyberCash, Inc. que viria a ser um serviço de pagamento pela internet para ser utilizado no comércio eletrônico, chegando a abrir capital em 1996. Por meio da empresa, era possível que os consumidores fizessem uso de uma carteira de software que aceitava pagamentos online a comerciantes. Expandiu, comprando a empresa ICVerify em 1998, porém, por problemas nos processos de funcionamento (duplicação de pagamentos e ataque hacker), acabou pedindo processo de falência em 2001, sendo comprada pela empresa VeriSign (SIDHU, 2021).

Entre outros projetos de moedas eletrônicas, têm-se historicamente o E-Gold, criado em 1996 pelo Dr. Douglas Jackson e Barry Downey, que visava ser vinculado à posse de ouro. Dessa forma permitiu que os indivíduos fizessem a transferência da propriedade de ouro entre si. Entretanto, o sistema de Jackson e Downey foi posteriormente usado para lavar dinheiro e manter anonimato em atividades criminais (REIFF, 2022). Na sequência, mais detalhes sobre os problemas naturais associados ao anonimato digital e seu uso em atividades ilegais.

Em 1997 o cientista da computação Nick Szabo divulgou o artigo *Formalizing and Securing Relationships on Public Networks* (formalizando e assegurando relacionamentos em redes públicas, tradução livre), onde viria a definir a base para o surgimento de formalização de contratos totalmente digitais, substituindo assim a necessidade escrita em papel. Como afirma Szabo: “a ideia básica por trás dos contratos inteligentes é que muitos tipos de cláusulas contratuais (como garantia, fiança, delimitação de direitos de propriedade etc.) podem ser embutidos no hardware e software com que lidamos, de forma a encarecer a quebra de contrato (se desejado, às vezes de forma proibitiva) para o infrator”, tradução livre. Com o artigo Szabo demonstrou que uma moeda digital só faria sentido caso a mesma possa ser usada na liquidação de contratos (SZABO, 1997).

Também em 1997 o criptógrafo e chypherpunk Adam Back, por meio de um e-mail (BACK, 1997), veio a propor um sistema que seria a base do Bitcoin e uma série de outras criptomoedas. O modelo de certificação e autenticação de dados por meio da prova de trabalho (Proof-of-Work ou PoW). Isso foi feito quando Back anunciou o Hashcash, como uma forma

de limitar o número de spam em e-mails e ataques de negação de serviço (DoS), utilizando um algoritmo criptográfico que necessita de uma quantidade mensurável de trabalho computacional para calcular. Assim, a verificação da autenticidade se mostra quando há um gasto com ciclos de computação da GPU no cálculo do carimbo data/hora. Em 2002 o Hashcash foi formalmente publicado em um artigo intitulado *Hashcash - A Denial of Service Counter-Measure* (Hashcash - Uma contramedida de negação de serviço, tradução livre) (BACK, 2002).

Em 1998, Nick Szabo desenvolveu o projeto de moeda digital descentralizada denominada “Bit Gold”. Sua estrutura de funcionamento fazia uso de um sistema próprio de registro de transações e com prova de trabalho (Proof-of-Work), que necessita que as transações sejam verificadas por meio da ação computacional, evitando com isso que a rede seja atacada com *spams* e ataques DoS (negação de serviço). O Bit Gold nunca foi implementado, mas foi considerado um precursor direto da arquitetura do Bitcoin, segundo o próprio Satoshi Nakamoto. Visto que era preciso um poder de processamento do computador para resolver quebra-cabeças criptográficos, servindo para verificar e carimbar novas moedas (SHARMA, 2021). No mesmo ano, Szabo publicou o ensaio *Secure Property Titles with Owner Authority* (títulos de propriedade seguros com a autoridade do proprietário, tradução livre), com a ideia de criar um banco de dados de títulos distribuído e seguro como uma forma para proteger os títulos de propriedade usando uma rede pública (SZABO, 1998).

Ainda em 1998, o engenheiro da computação Wei Dai publicou o *b-money*, um artigo que possuía o objetivo de criar uma criptomoeda em conformidade com a filosofia criptoanarquista, onde *a ameaça de violência é impotente porque a violência é impossível, e a violência é impossível porque seus participantes não podem ser vinculados a seus nomes verdadeiros ou localizações físicas*. Para isso o autor cria dois protocolos: um impraticável, pois faz uso intenso de um canal de transmissão anônimo síncrono e ininterrupto; e outro mais prático, utilizando subprotocolos. Além de propor uma solução para a criação de novas unidades da moeda, por meio de um sistema de leilão custoso.

2.4 UTILIZAÇÃO PRÁTICA

Em 1999 foi fundado o Napster, um software que permitia do download de arquivos de áudio digital por meio da internet via pessoa-a-pessoa (peer-to-peer, ou P2P). No mesmo ano o site Beenz.com (entre outros) disponibilizou um sistema de pontuação por compra no site por meio de uma moeda digital, a *beenz*. Porém foi apenas uma forma de aproveitar a tendência das moedas digitais, tendo, assim, fracasso logo em seu lançamento. Em 2001 ocorre a quebra

da bolha Dot-Com, mostrando ainda mais os problemas dentro das finanças tradicionais. No mesmo ano lança-se o BitTorrent, um sistema que permite o compartilhamento de arquivos via ponto a ponto (P2P), pelo cypherpunk Bram Cohen, demonstrando a ascensão de programas e protocolos individuais, sem a necessidade de centralização (SIDHU, 2021).

No período de 2000 a 2004, vários jogos online surgiram com um ambiente multijogador e com economia interna, a exemplo tem-se os jogos *Second Life* que criou sua própria moeda virtual chamada de Linden Dollars (L$), e o *World of Warcraft*, com o *gold* (ouro). Porém ambos os jogos sofreram com um problema monetário: inflação. Visto que ocorria problema de gasto duplo e geração infinita de moeda dentro dos jogos. Isso não era só um problema para uma economia virtual, mas um desafio matemático e computacional. Visto que se uma criptomoeda contém gasto duplo, ela acaba por duplicar a base monetária e causar inflação, levando a mesma a perder seu valor e propriedade monetária (reserva de valor) (SIDHU, 2021). Para solucionar esse problema, Hal Finney, um desenvolvedor de software que trabalhou na corporação PGP (*pretty good privacy*), desenvolveu a Prova de Trabalho Reutilizável (*Reusable Proof-of-Work*, RPoW), resolvendo o problema do gasto duplo por meio de um sistema que mantinha a propriedade dos tokens registrados em um servidor confiável, não mais em posse do próprio usuário (FINNEY, 2004).

Mais uma inovação criptográfica foi a criação do Contrato Ricardiano, apresentado em 1996 por Ian Grigg, mas publicado oficialmente em 2004 no artigo *The Ricardian Contract* (O Contrato Ricardiano, tradução livre). Este contrato permite que um acordo legal possa ser verificado e executado em um software, de forma que seja legível por humanos utilizando uma máquina, de modo que advogados e as partes contratantes possam entender o mesmo (GRIGG, 2004).

Por fim, tem-se em 2001 a criação da Liberty Reserve por Arthur Budovsky e Vladimir Kats, um sistema de moeda digital anônimo que atendeu mais de um milhão de clientes em todo o mundo e realizou um total de doze milhões de transações anuais. O serviço permitia transferir dinheiro para outros usuários utilizando apenas um nome, endereço de e-mail e data de nascimento. Porém não havia processos de checagem de autenticidade da identidade de seus usuários e o sistema era utilizado em processos de lavagem de dinheiro, o que acarretou na prisão de Budovsky em 2016 a vinte anos de prisão (CHEN, 2020).

2.5 BASE FILOSÓFICA E POLÍTICA

As moedas digitais que atualmente estão em expansão possuem um passado filosófico em comum, remontando a uma filosofia liberal e posterior anarquista e anarco-capitalista. Sendo a primeira crítica econômica ao sistema de base monetária baseado em um sistema fiat, ou seja, centralizado à presença de um Estado regulador e criador de moeda, vindo do economista ganhador do Nobel de economia de 1974, Friedrich August von Hayek. Em 1976 Hayek publicou o livro *The Denationalisation of Money*, que viria a ser expandido e revisado em 1978 como *Denationalisation of Money: The Argument Refined*.

No livro, o autor defende a tese de que em um sistema monetário competitivo, com empresas privadas desenvolvendo suas próprias moedas, haveria uma tendência natural a uma convergência para um ou um número reduzido de padrões monetários. Tal tese entra em concordância com a Teoria Austríaca dos Ciclos Econômicos desenvolvido por Eugen von Böhm-Bawerk, Ludwig von Mises e Hayek (MAHONEY, 2008). A teoria afirma que a presença de um banco central interventor, que expande a base monetária e com isso muda as taxas de juros da economia acabam por gerar ciclos econômicos que levam a crises. Dessa forma, sem a presença de um órgão centralizador, como o Banco Central, levaria a um sistema de taxas de juros naturais que trariam uma estabilização nos ciclos econômicos, sem gerar distorções artificiais por conta da expansão ou retenção monetária (HAYEK, 2011).

A segunda base para a filosofia ética basilar das criptomoedas, Bitcoin especificamente, foram os livros *What Has Government Done to Our Money?* de 1963 e *Ethics of Liberty* de 1982, ambos do economista, historiador e filósofo da Escola Austríaca de Economia, Murray N. Rothbard. No primeiro livro o autor é predecessor do já mencionado livro de F.A. Hayek, demonstra como o Governo, enquanto instituição, privou a população de poder livremente escolher uma moeda que individualmente melhor lhe suprissem e impediu a livre competição monetária. Com isso o autor mostra que para uma moeda ter qualidade, ela precisa ser considera como um bem qualquer, tal como maçãs e bananas, e estar em possibilidade de teste de mercado (ROTHBARD, 2010).

O segundo livro de Rothbard cria a base filosófica do Movimento Libertário e Anarco-capitalista, mostrando em obra a figura da instituição estatal como um violador natural dos direitos naturais do ser humano, visto que para o Governo existir é preciso que o mesmo invada a propriedade privada (captação de recursos por meio de impostos, ou seja, roubo com ameaça de violência em caso de negação) e infira contra a liberdade individual (proibição de

criar livremente moedas e outros bens que são considerados “de interesse nacional”). (ROTHBARD, 2013) O mesmo afirma:

> Nosso exemplo do carro roubado nos permite enxergar imediatamente a injustiça do atual conceito legal do “título de crédito”. Na lei atual, o carro roubado de fato seria devolvido ao dono original sem nenhuma obrigação da parte dele de recompensar o atual detentor do título injusto. Mas o estado designou certos bens como “objetos negociáveis” (e.g., cédulas de dinheiro) cuja posse supõe-se ser do recebedor ou do comprador não-criminoso, e cuja devolução à vítima não pode ser forçada. As legislações peculiares também têm transformado os empenhadores em uma classe semelhantemente privilegiada; de modo que, se Bruno rouba uma máquina de escrever de Luiz, e então a empenha com Roberto, o empenhador pode não ser obrigado a devolver a máquina de escrever ao seu justo dono, Luiz (ROTHBARD, 2010, p. 120).

Com o livro, Rothbard afirma a incoerência legal que existe entre os direitos naturais dentro de um sistema de livre mercado total e com a presença de um Estado. Sendo filosoficamente necessário que não exista um Estado para que os direitos naturais sejam plenamente respeitados. E com isso, o mesmo demonstra que o dinheiro deve ficar separado de uma instituição governamental, podendo ser criado e comercializado como um bem comum (ROTHBARD, 2010).

No ano de 1988, o engenheiro eletrônico Timothy C. May publicou o escrito *The Crypto Anarchist Manifesto* (O Manifesto Cripto-Anarquista, tradução livre), introduziu as bases da anarquia digital, a qual os indivíduos passam a ter suas liberdades políticas, econômicas e de privacidade respeitadas por meio do uso de sistemas descentralizados e anônimos. May também aponta que os governos irão acusar essas tecnologias como ferramentas para o uso de traficantes de drogas e sonegadores de impostos, porém, que de forma inevitável elas serão usadas, pois trazem consigo a liberdade e privacidade plena (MAY, 1988).

May juntou-se a um grupo de outros criptógrafos, matemáticos e hackers que trouxeram consigo um know-how político, tecnológico, econômico, filosófico etc. Sendo alguns destes já mencionados anteriormente, como Adam Back, Hal Finney e Philip Zimmermann. Eles defenderam o uso generalizado de forte criptografia e de tecnologias que garantissem a privacidade como uma forma de mudança político-social (SIDHU, 2021). E no ano de 1993, o matemático e programador Eric Hughes publica *A Cypherpunk's Manifesto* (manifesto de um cypherpunk, tradução livre), mostrando os pilares do que viria a ser o Bitcoin,

sendo estes: privacidade nas comunicações, anonimato e uso de pseudônimos, transações econômicas totalmente anônimas e utilização de criptografia (HUGHES, 1993).

O último trabalho anterior à criação do Bitcoin foi lançado pelo economista alemão da Escola Austríaca de Economia, Jörg Guido Hülsmann em 2008. Com o título *The Ethics of Money Production* (A Ética da Produção do Dinheiro, tradução livre), a obra veio a trazer um complemento aos já mencionados trabalhos de Hayek e Rothbard, com a tese de que o governo não deve ser responsável pela criação e manutenção da moeda, visto que o passado histórico demonstrou que essa entidade violou os direitos individuais e foi responsável por gerar inflação e instabilidade à moeda (SIDHU, 2021). Ele narra a queda de moedas que foram nacionalizadas, até o ponto onde ocorreu hiperinflação causada pelos governantes. E autor expõe de forma certeira o boom imobiliário americano que viria a ocorrer no mesmo ano:

> Considere o atual boom imobiliário dos Estados Unidos (2006). Muitos americanos estão totalmente convencidos de que o setor imobiliário americano é a única aposta certa na vida econômica. Não importa o que aconteça no mercado de ações ou em outros estratos da economia, os imóveis vão subir. Eles acreditam ter encontrado uma bonança, e os números históricos confirmam isso. É claro que essa crença é uma ilusão, mas a característica de um *boom* é precisamente que as pessoas jogam fora quaisquer considerações críticas. Eles não percebem que seu produtor de dinheiro – o FED – possivelmente já entrou nos estágios iniciais da hiperinflação, e que a única razão pela qual isso tem sido praticamente invisível é que a maior parte do novo dinheiro foi exportado para fora dos EUA. Os preços monetários aumentaram tremendamente acima do nível que teriam alcançado sem a produção implacável de dólares, mas o aumento absoluto do nível de preços domésticos (conforme medido pelos números do CPI) tem sido relativamente moderado até agora. No entanto, assim que os estrangeiros diminuírem suas compras de dólares americanos, os preços domésticos começarão a subir e, em seguida, a hiperinflação se aproxima. (Tradução livre) (HÜLSMANN, 2008, p. 171).

2.6 CRISE DE 2008 E NASCIMENTO DO BITCOIN

No dia 31 de outubro de 2008, a pessoa ou entidade anônima com o pseudônimo Satoshi Nakamoto (2008) enviou ao fórum de discursão online, intitulado *The Cryptography Mailing*, o whitepaper do Bitcoin, *A Peer-to-Peer Electronic Cash System*, que veio com a proposta de eliminar intermediários financeiros em um sistema monetário. Para isso foi preciso solucionar um problema matemático que fez outros projetos de moedas digitais anteriores fracassarem, este foi o problema do gasto duplo, com o qual as moedas eram arquivos de

computador, estes que podiam ser copiados, gerando mais moedas na economia. Esse problema foi solucionado com a implementação de uma *blockchain* ponta-a-ponta, criando um sistema de segurança a qual todas as transações são salvas em uma cadeia sequencial totalmente pública à visualização (NAKAMOTO, 2008).

Em 03 de Janeiro de 2009, a rede do Bitcoin foi lançada, surgindo assim o primeiro arquivo computacional que possibilitou o surgimento da criptomoeda. Foi definido de forma arbitrária o valor de 21 milhões de moedas possíveis para criação, por meio do processo de mineração, que é a validação das transações por meio de um bloco da *Blockchain*. Além da remuneração por esse custo computacional, que no período foi a taxa de transação e 50 Bitcoins por bloco, o sistema de aumento da dificuldade computacional para equilibrar a rede e a redução pela metade da quantidade ofertada de Bitcoins a cada dez mil blocos minerados (VELLEDA, 2021).

Associado ao ouro, como um "ouro digital", o Bitcoin é armazenado na Blockchain e a custódia ao acesso deste, por meio das chaves privadas de acesso, são inteiramente de responsabilidade do investidor que o possui. Remove-se assim intermediários financeiros e possibilita liberdade monetária completa, além de ser de fácil envio de uma carteira à outra, o que é menos custoso quando comparado ao ouro. E com o avanço do Bitcoin e de demais moedas digitais, em especial a Ethereum, algumas empresas (ex.: Ledger e Trezor) possibilitaram o armazenamento das chaves de maneira segura em um dispositivo não conectado à internet, este é chamado de *hardware wallet*. Necessitando que o investidor apenas memorize ou salve em um local seguro sua *Seed Phrase*¸ que é uma série de palavras que a carteira cria durante sua fase inicial de configuração, usando a codificação BIP44 ou BIP49 (COINBASE, 2021).

Ao analisar o resultado de perda de poder de compra da população por meio da inflação, causada pela expansão monetária, constata-se que os governos e bancos centrais em geral destroem com o decorrer do tempo o valor de suas moedas, isso é visto em especial no cenário econômico Brasileiro, o qual por mais de quatro décadas (Cruzeiro até o Real) era comum inflações anuais superiores a 16% e durante a hiperinflação, década de 1980 à 1990, superiores a 200%. E com o Real o mesmo vem ocorrendo desde sua implementação em 1994, perdendo, de 08/1994 a 12/2021, aproximadamente 568,19% de seu poder de compra. Assim, a proposta de limite máximo de Bitcoins passíveis de serem minerados possibilita uma segurança financeira que se assemelha ao ouro, além de retirar o poder controlador de um intermediário financeiro de usar da moeda para ganhos próprios (BRASIL, 2022).

No processo de análise de longo prazo, desde a primeira troca realizada de forma física em 22 de maio de 2010 de 10 mil Bitcoins por 2 pizzas (*Pizza Day*), o preço do Bitcoin sobe de forma exponencial (MATOS, 2020). Saindo de U$ 0,007 para a alta histórica, em 08 de novembro de 2021, de U$ 66.930. Mostrando um comportamento de deflação econômica quando analisado com moedas fiat (INVESTING, 2022).

Por possuir um limite de criação monetária pré-definido e com uma taxa de criação conhecida, 10 mil blocos a cada 4 anos em média, o autor anônimo autointitulado de PlanB, com a utilização de técnicas estatísticas criou o Modelo *Stock-to-Flow*, o qual se baseia no limite máximo que o Bitcoin pode alcançar, 21 milhões, sua redução de recompensa de mineração a cada 4 anos e com a tendência natural dos Estados expandirem suas reservas monetárias. De acordo com PlanB:

> *The predicted market value for bitcoin after May 2020 halving is $1trn, which translates in a bitcoin price of $55,000. That is quite spectacular. I guess time will tell and we will probably know one or two years after the halving, in 2020 or 2021. A great out of sample test of this hypothesis and model* (PLANB, 2019).

Assim, há uma visão de que o Mercado ainda tende a crescer de forma ascendente, podendo vir a chegar, de acordo com PlanB (2019), a U$ 100 trilhões de valor de mercado em um momento futuro. E com o estudo feito por Hong (2017), por meio de uma série temporal do período de 2013 a 2015, com a adição de uma parcela pequena de investimento em Bitcoin, este pode ajudar a equilibrar a equação risco-retorno da carteira. Mostrando evidência que investidores podem aproveitar desse ativo como forma de diversificação.

2.7 NOVAS TECNOLOGIAS

O Bitcoin foi o resultado de uma evolução criptográfica, filosófica, econômica e política de mais de trinta anos. É possível analisar em seu esqueleto as tecnologias que possibilitaram a criação da Blockchain, com a utilização do sistema de prova de trabalho (Proof-of-Work), as árvores de Merkle e as demais formas de criptografar a identidade dos indivíduos, como as assinaturas cegas e as chaves públicas e privadas. Porém, o Bitcoin passou a ser uma criptomoeda que serve de *benchmark* (ponto de referências) para as demais criptomedas, visto

que seu valor de mercado é 2,3 vezes maior que a segunda criptomoeda mais utilizada, a Ethereum (valor de mercado em 10 de out. de 2022)[2].

Assim, a partir da tecnologia *blockchain* diversos projetos não só monetários, mas também contratuais (*smart contracts*) foram desenvolvidos como tentativas de solucionar problemas que o Bitcoin não disponibiliza ou ainda está sendo desenvolvido pela comunidade. É o caso da Ethereum, que permite que dentro do seu ecossistema (sua *blockchain*) ocorram contratos de moedas estáveis (*stablecoins)*, corretoras descentralizadas, sistema de empréstimos diretos, finanças descentralizadas (DeFi), Fan Tokens (ex.: moedas digitais de times de futebol), tokens não fungíveis (*non-fungible token*, ou NFT, ex.: obras de arte), jogos descentralizados e uma série de outros projetos. Assim, o lastro inicial das criptomoedas passou a ser variável, dependendo diretamente da fundamentação do projeto e suas perspectivas para o futuro.

2.8 PROBLEMAS E REGULAMENTAÇÃO BRASILEIRA

Como toda ferramenta, as criptomoedas podem ser utilizadas para resolver problemas complexos e serem disruptivas ao sistema *mainstream* e ao mesmo tempo podem ser usadas para usos criminais, tais como lavagem de dinheiro, recebimento de pagamento de produtos ilícitos (ex.: drogas e armamento não legalizados), aplicação de pirâmides financeiras, *Pump and Dump* e chantagem. Com a adoção midiática das criptomoedas, de acordo com a *Global Crypto Adoption Index* de 2022, o Brasil passou à sétima posição mundial em transações (CHAINALYSIS, 2022). Gerando oportunidade para que criminosos criem golpes utilizando criptoativos (ou fingindo o seu uso) em pessoas pouco instruídas e que buscam lucros rápidos e altos.

É o caso do golpe aplicado por Glaidson dos Santos, mais conhecido por "Faraó dos Bitcoins" e Mirelis Yoseline Diaz Zerpa, utilizando a empresa GAS Consultoria & Tecnologia LTDA. Glaidson prometia retornos mensais de 10% sobre o montante investido, o que criou um leque de clientes que aplicaram na empresa recursos que chegaram a movimentar R$ 38 bilhões em seis anos. Entretanto, tudo não passou de um esquema de pirâmide financeira, com o qual os envolvidos recebiam os recursos dos clientes, porém não aplicavam em criptomoedas (HERINGER; SOUZA, 2021).

No dia 11 de outubro de 2022, a Comissão de Valores Mobiliários divulgou o Parecer de Orientação 40, que consolida o entendimento da Autarquia sobre as normas que são

[2] Dado obtido no site *CoinMarketCap*, disponível em: <*coinmarketcap.com/currencies/ethereum/*>.

aplicáveis aos criptoativos que forem considerados valores mobiliários, além de apresentar os limites de atuação do regulador. No documento, caracteriza-se os criptoativos como:

> [...] ativos representados digitalmente, protegidos por criptografia, que podem ser objeto de transações executadas e armazenadas por meio de tecnologias de registro distribuído (*Distributed Ledger Technologies* – DLTs). Usualmente, criptoativos (ou a sua propriedade) são representados por *tokens*, que são títulos digitais intangíveis. (BRASIL, 2022)

Afirma também que *a tokenização em si não está sujeita à prévia aprovação ou registro perante a CVM.* Entretanto, *tanto os emissores quanto a oferta pública de tais tokens estarão sujeitos à regulamentação aplicável*. [...] *Da mesma forma, ainda que se utilizem de novas tecnologias, a administração de mercado organizado para negociação dos tokens, bem como os serviços de intermediação, escrituração, custódia, depósito centralizado, registro, compensação e liquidação de operações que envolvam valores mobiliários estarão sujeitos às regras aplicáveis a essas atividades* (BRASIL. 2022). Assim,

> Ainda que os criptoativos não estejam, expressamente, incluídos entre os valores mobiliários citados nos incisos do art. 2º da Lei 6.385, o Parecer de Orientação 40 indica que os agentes de mercado devem analisar as características de cada criptoativo, com o objetivo de determinar se é valor mobiliário, o que ocorre quando: (i) é a representação digital de algum dos valores mobiliários previstos taxativamente nos incisos I a VIII do art. 2º da Lei 6.385 e/ou previstos na Lei 14.430 (i.e., certificados de recebíveis em geral); ou (ii) se enquadra no conceito aberto de valor mobiliário do inciso IX do art. 2º da Lei 6.385, na medida em que seja contrato de investimento coletivo. (BRASIL, 2022)

Após o exposto, a Autarquia divide os tokens segundo uma abordagem funcional em taxonomia que servirá para indicar o seu tratamento jurídico. Que a início, seguirá as seguintes categorias: Token de Pagamento (*cryptocurrency* ou *payment token*): busca replicar as funções de moeda, notadamente de unidade de conta, meio de troca e reserva de valor; (ii) Token de Utilidade (*utility token*): utilizado para adquirir ou acessar determinados produtos ou serviços; e (iii) Token referenciado a Ativo (*asset-backed token*): representa um ou mais ativos, tangíveis ou intangíveis. Sendo o último podendo ou não ser um valor mobiliário e um criptoativo pode ou não se enquadrar em mais de uma das categorias (BRASIL, 2022).

No dia 29 de novembro de 2022 a Proposta de Lei nº 4401 de 2021 foi aprovada pelos Deputados Federais, estabelecendo o Banco Central do Brasil (BACEN) como órgão nacional e responsável pela regulamentação. Na mesma, afirma que as empresas irão precisar

de licença para funcionar no país, por meio de critérios com o qual o BACEN ainda deverá criar. Com isso, a maioria das plataformas de trocas (exchanges), fintechs e bancos entraram em concordância, afirmando que a lei traz maior segurança jurídica e permite novas oportunidades no mercado (ROCHA, 2022).

Porém, a aprovação da PL não entrou em concordância com todo o mercado, possuindo pontos críticos que foram denunciados por nomes como Felipe Escudero, influenciador do canal BitNada, Alex Nagatome, fundador da Fort Exchange, Daniel Coquieri, CEO da Liqi e Ray Nasser e Rudá Pelline, da Arthur Mining. O primeiro afirma que há dois pontos chamativos: que os Deputados não possuíam conhecimento sobre a pauta, referindo, por exemplo, Bitcoin como “Bitcom” e segundo, por haver a necessidade de retirar uma licença junto ao BACEN, o mesmo gera um lobby e restringe a concorrência. Os segundo e terceiro, afirmam que o projeto pode gerar o efeito reverso que pretende, pois retira o artigo de segregação patrimonial, que separava o patrimônio das empresas do dos clientes e gera maior burocracia para as negociações, dificultando a compra. Os últimos apontam para o perigo para a criação de lobby de mineração de criptomoedas, por conta da retirada da cláusula de isenção de impostos de importação para os mineradores (ROCHA, 2022).

E após a aprovação da PL, que irá passar por sanção presidencial, a Comissão de Valores Mobiliários por meio de seu presidente, João Pedro Nascimento, afirmou que irá ser “muito ativa” na regulamentação. Nascimento afirma que as regras para o mercado de criptomoedas serão “pouco invasivas” e deverão focar no incremento da governança e na separação patrimonial (VASCONCELOS, 2022).

3 INVESTIMENTOS

3.1 DIVERSIFICAÇÃO

Os investimentos possuem um risco, este que pode ser definido de diversas maneiras, tais como: os fundamentos do ativo perderem o valor e a probabilidade da não ocorrência do que se espera, como o ativo perder/aumentar de preço acima do esperado. E correlacionado ao risco, o investidor exige um retorno que seja adequado ao risco que está incorrendo, visto que o mesmo poderia alocar seu capital em ativo livre de risco (*Risk Free*). Dessa forma, quanto maior o risco do investimento, maior deverá ser o retorno esperado do ativo e o inverso também é verdadeiro.

Em 1952, o economista estadunidense Harry M. Markowitz publica o artigo *Portfolio Selection* (seleção de carteira, tradução livre). Nele o autor veio a demonstrar, a posteriori, uma citação antiga presente no O Mercado de Veneza, do clássico romancista William Shakeaspere, “não coloque todos os ovos em uma mesma cesta”. Isso foi demonstrado por meio de técnicas de média-variância, com o qual é possível que o investidor consiga encontrar uma carteira com um retorno esperado para *n* tipos de variância, necessitando apenas que o mesmo esteja em condições de aceitar níveis diversos de volatilidade (MARKOWITZ, 1952). Segundo o autor, mesmo que

> Suponha que um investidor diversifique entre duas carteiras (ou seja, se ele colocar parte de seu dinheiro em uma carteira, e o restante em outra. Um exemplo de diversificação entre carteiras é a compra de ações de duas empresas de investimento diferentes). Se as duas carteiras originais tiverem variância igual, normalmente a variância da carteira resultante (composta) será menor que a variância de qualquer uma das carteiras originais [MARKOWITZ, 1952].

Assumido o portfólio, com o uso da correlação e da covariância (MARKOWITZ, 1952) é possível medir a comovimentação dos retornos. Dessa forma, é possível que dois grupos de ativos fiquem interligados ao mesmo tempo abaixo ou acima da média, causando assim uma correlação positiva (MOUTINHO, 2019). O inverso também ocorre, se a movimentação for em uma direção oposta a correlação será negativa, visto que uma fica acima da média, e a outra tenderá a ficar abaixo dela (MOUTINHO, 2019) (BERK; DEMARZO, 2009). Assim, investimentos variados em ativos com uma correlação mais baixa tendem a ser mais racionais para o investidor (MARKOWITZ, 1952).

A força da relação entre os ativos se calcula por meio de sua correlação entre retornos, com evidência aos riscos comuns e tendências de movimentação juntas (MOUTINHO, 2019). Assim, correlação próximo de +1 demonstra que os retornos tendem a ir juntos como consequência de eventos similares; correlação igual a 0, não há tendência; correlação -1, as movimentações vão em direção oposta (MOUTINHO, 2019) (BERK; DEMARZO, 2009). Por fim, se usa o Índice de Sharpe, que é obtido pelo retorno do portfólio descontado da taxa de retorno de ativo livre de risco, dividido pelo desvio-padrão da carteira (MOUTINHO, 2019; BERK; DEMARZO, 2009).

Markowitz (1952) afirma que *o investidor gostaria (ou deveria) selecionar uma daquelas carteiras que dão origem às combinações (E, V) indicadas como eficientes na figura; isto é, aquelas com mínimo V para dado E ou mais e máximo E para dado V ou menos.* Ou seja,

todos os pontos presentes na combinação eficiente E, V são preferíveis àqueles que estão fora do sistema.

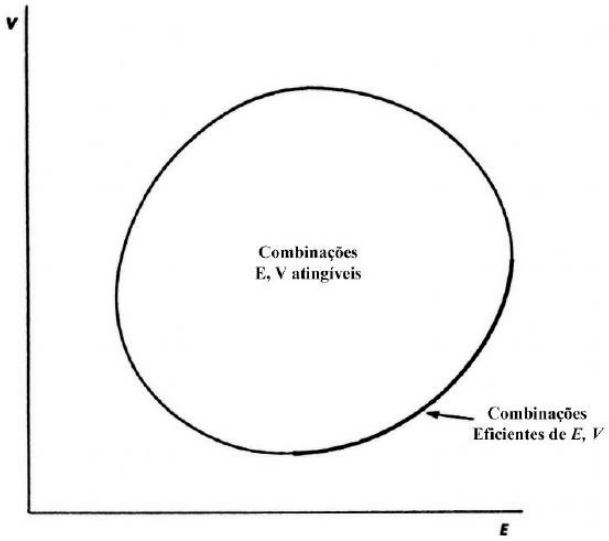


FIG. 3: Figura traduzida do artigo *Portfolio Selection* (MARKOWITZ, 1952, p.82)

3.2 ANÁLISE DOS DADOS

É possível fazer uso da Linha de Alocação de Capital [*Capital Allocation Line* (CAL)], que é uma linha criada em um gráfico contendo todas as possíveis combinações de ativos que possuem ou não risco. No mesmo gráfico, pode-se observar o retorno que os investidores conseguem obter, trazendo para si um nível de risco, e a inclinação da linha, considerada como uma relação recompensa-variabilidade. O retorno esperado da carteira é obtido por meio de uma média ponderada dos retornos esperados de cada ativo individual com seu devido peso na carteira, como visto na fórmula:

$$E(Rp) = w_1 E(E_1) + w_2 E(R_2) \quad (1)$$

onde w_1, w_2 são os respectivos pesos para os dois ativos, com $w_1 + w_2 = 1$, e $E(R_1)$, $E(R_2)$ são os retornos esperado dos ativos 1 e 2, respectivamente. E a variância da mesma é obtida com a fórmula

$$Var(R_p) = w_1^2 Var(R_1) + w_2^2 Var(R_2) + 2w_1 w_2 Cov(R_1, R_2) \quad (2)$$

onde $Cov(R_1, R_2)$ é a covariância dos dois retornos dos ativos (CFI, 2022).

Com o uso de ativos livres de risco, normalmente títulos governamentais de países com baixo risco-país, pode-se demonstrar o retorno esperado de uma carteira completa como sendo $E(R_c) = w_p E(R_p) + (1 - w_p)R_f$ e a variância sendo $Var(R_c) = w_p^2 Var(R_p), (R_c) = w_p(R_p)$, onde w_p representa o peso alocado nos ativos de risco e $E(R_c) - R_f$ sendo o excesso do retorno esperado da carteira. Se adicionarmos $E(R_c)$ pela fórmula anterior, obtemos $w_p(E(R_p) - R_f)$. Sendo o desvio padrão da carteira completa dado como $\sigma(R_c) = w_p \sigma(R_p)$, temos $w_p = \sigma(R_c)/\sigma(R_p)$. Assim, temos que, para cada carteira completa:

$$\frac{E(R_c) - Rf}{\sigma(R_c)} = \frac{[\cancel{w_p}(E(R_p) - Rf)]}{\cancel{w_p}\sigma(R_p)} = \frac{(E(R_p) - R_f)}{\sigma(R_p)} \quad (3)$$

ou, $E(R_c) = R_f + S_p \sigma(R_c)$, onde $S_p = \frac{(E(R_p) - R_f)}{\sigma(R_p)}$. Onde a linha $E(R_c) = R_f + S_p \sigma(R_c)$ é a linha de alocação de capital (CAL) e sua inclinação é causada por meio do Índice de Sharpe, S_p, também nomeado como Índice de recompensa para risco. Este tem como função medir quanto muda o retorno esperado devido a uma mudança no desvio padrão adicional. Por fim, temos que uma carteira ideal é aquela onde a linha de alocação de capital é tangente à fronteira eficiente, como visto na Figura 4. Visto que neste ponto é possível alcançar os maiores retornos esperados por unidade adicional de risco (CFI, 2022).

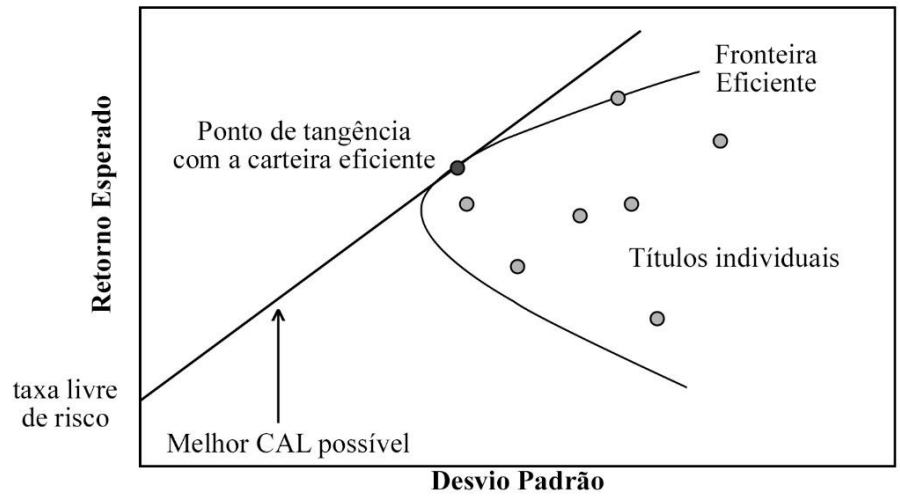


FIG. 4: Fronteira Eficiente de Markowitz. Elaboração própria

3.3 EXEMPLOS DE MAXIMIZAÇÃO DE CARTEIRA COM CRIPTOATIVOS

Ao analisar a literatura, encontrou-se trabalhos que corroboraram para a inclusão de Bitcoin no portfólio, de forma a causar um efeito positivo na relação risco-retorno, é o caso dos trabalhos de Moutinho (2019), Li (2021) e Shellinger (2020):

De acordo com Moutinho (2019), que fez uma pesquisa quantitativa com 48 observações mensais, no período entre janeiro de 2014 a dezembro de 2017, os resultados apontaram que que os retornos dos portfólios são maiores em carteiras contendo o Bitcoin para os anos de 2015, 2016 e 2017, enquanto que em 2014 não se teve diferenças, exatamente o ano em que os retornos do Bitcoin foram negativos. Assim, o acréscimo do Bitcoin em um portfólio de investimento se mostrou vantajosa, permitindo trazer uma melhor otimização da carteira.

Li (2021), por meio do *framework* de média-variância de Markowitz (1952), avaliou se o Bitcoin poderia contribuir para uma carteira eficiente. Obteve o resultado que Bitcoin tem uma tendência enorme de melhorar o perfil de risco-retorno do investidor. Tanto para a venda a descoberto que era ou não restrita.

Com o uso do Índice Sharpe e posterior comparação com estratégias de portfólio alternativas, Schellinger (2020), obteve resultados que uma carteira de utilidade máxima de moedas, com aversão ao risco de $\lambda = 10$, supera as estruturas alternativas.

4 METODOLOGIA

4.1 COLETA DE DADOS E SELEÇÃO DE AMOSTRA

Foi elaborada uma pesquisa descritiva e quantitativa, com um universo de 1034 observações diárias, no período de 01 de janeiro de 2020 a 31 de outubro de 2022. Foram coletadas as séries históricas de cada ativo por meio site *Yahoo! Finance*, que armazena todos os dados de preços de fechamento ajustados. As variáveis estudadas foram: (a) Bitcoin (BTC); (b) Ethereum (ETH); (c) Ripple (XRP); (d) Cardano (ADA); (e) Polygon (MATIC); (f) Litecoin (LTC); e (g) Chainlink (LINK).

Os criptoativos foram escolhidos de maneira aleatória, porém, seguindo a premissa de que todos deveriam ter uma Oferta Inicial de Moeda (ICO) ou Oferta Inicial de Exchange (IEO) anterior ou a partir de 01 de janeiro de 2020, para que a base de dados possuísse o mesmo número de dias. Segundo, apesar da escolha ser aleatória, foi privilegiado as maiores moedas em valor de mercado (*market cap*), visto sua maior liquidez para o investidor.

Visto os estudos apresentados no capítulo 3.3, buscou-se utilizar uma base dados atualizada, arbitrária e aleatória, com intuito de evitar juízo de valor e escolhas de períodos que beneficiassem resultados positivos à alocação do ativo em estudo para a carteira maximizada. Porém, o mesmo engloba a crise provocada pela pandemia de COVID-19. Nesse cenário, a volatilidade de todos os ativos, incluindo as criptomoedas, cresceu. Portanto, será possível observar o comportamento das carteiras diante deste cenário de cisne negro (crise sistêmica).

4.2 TRATAMENTO DE DADOS E PROCEDIMENTOS UTILIZADOS

Por meio de dados coletados no período de janeiro de 2020 a outubro de 2022, realizar-se-á os cálculos dos retornos de todos os ativos, assim como seus desvios-padrão, correlações e covariâncias. Serão elaborados alguns cenários: o de pesos iguais (*equal weights*); o com variação mínima (*minimal variation*); o portfólio maximizado, que assim como no *minimal variation*, terá seus pesos com flutuação livre; e um com pesos totalmente aleatórios (*randarray*). Em todos os casos não irá ser levado em conta alavancagem financeira, de forma que a soma de todos os pesos será igual a 1 (ou 100%) e os mesmos com valores sendo maiores ou iguais a 0. Para encontrar os resultados será feito uso de um recurso de solução automática por premissas delimitadas disponível em um software de gerenciamento de dados.

Com a criação do portfólio com pesos aleatórios será elaborado uma base de dados com 150 mil combinações possíveis entre seu risco e retorno, possibilitando que seja possível criar graficamente a fronteira eficiente de Markowitz, analisar onde os cenários são observáveis e definir a *Capital Allocation Line* (CAL), que tangencia o portfólio eficiente. Como a CAL necessita do Índice de Sharpe o mesmo necessita de uma taxa de retorno de um ativo que seja livre de risco, logo, será escolhido a taxa de retorno da *Treasury Note* (T-Note) de 10 anos, considerado o ativo mais seguro do mundo.

4.3 COMPARAÇÃO COM FUNDOS DE INVESTIMENTO MULTIMERCADO

Após obter os resultados das carteiras estudadas, será feito a comparação com os retornos advindos de Fundos de Investimento Multimercado (FIMs) no ano de 2021. Retornos estes passíveis de visualização na Tabela 1.

Fundo	Retorno (%)
Esh Theta FI Mult	116,10%

Safra S&P FI Mult	40,03%
Itau Index Mult Estrategia Sp500 Usd Fc	38,13%
Trend Imobiliario Americano FI Mult	34,19%
BTG Pactual S&P 500 Brl FI Mult	31,14%
Sicredi Bolsa Americana FI Mult LP	30,55%
Brad Private Fc FI Mult S&P 500 Brl	30,23%

Tabela 1: Maiores retornos acumulados de fundos de investimento multimercado[3]. Elaboração própria.

5 RESULTADOS

5.1 RETORNOS

O primeiro passo foi calcular os retornos diários, a esperança dos retornos diários E(r), o desvio padrão, a variância e o Índice de Sharpe Modificado. O E(r) de cada ativo foi encontrado por meio de uma média aritmética da variação diária do ativo. A variação diária, por exemplo: $P_0 = 1000$ e $P_1 = 1100$, sua variação diária é igual a $rP = \frac{1100-1000}{1000} = 0{,}1$. Os resultados obtidos estão na Tabela 2, e de primeiro momento, pode-se constatar que o retorno diário esperado do Bitcoin e do Litecoin são próximos, os demais ativos, exceto a Polygon, possuem um retorno esperado diário maior, porém próximos, e a Polygon possui o maior retorno diário esperado.

Assim, pode-se inferir inicialmente que a combinação entre Litecoin e Bitcoin irá gerar um retorno esperado próximo, podendo ser motivo para trocar um dos ativos da carteira para elevar o retorno ou, como veremos adiante, elevar a diversificação dos ativos.

	BTC	ETH	XRP	ADA	MATIC	LTC	LINK
n	1034	1034	1034	1034	1034	1034	1034
E(r)	0,0018	0,0037	0,0029	0,0042	0,0071	0,0017	0,0036
σ	0,0383	0,0507	0,0641	0,0597	0,0806	0,0527	0,0650
σ²	0,0015	0,0026	0,0041	0,0036	0,0065	0,0028	0,0042
E(r)/σ	0,0461	0,0735	0,0445	0,0702	0,0878	0,0321	0,0552

Tabela 2: Informações sobre os ativos. Elaboração própria.

[3] Disponível em: <*einvestidor.estadao.com.br/mercado/fundos-acoes-multimercados-mais-rentaveis-2021*>

5.2 CORRELAÇÃO E COVARIÂNCIA

Com a variação dos preços dos ativos é possível criar uma matriz que intercorrelaciona suas variações individuais, a Matriz de Correlação. Ela demonstra o quão próximo um ativo está relacionado com o outro, sendo 1 completamente correlacionado, 0 sendo indiferentes ou independentes e -1 totalmente não correlacionados. Como analisado pela Tabela 3, constata-se que todos os ativos possuem uma correlação entre si próxima e positiva. Em destaque para os casos entre Bitcoin com Ethereum, Bitcoin com Litecoin e Ethereum com Litecoin, que possuem uma correlação acima de 0,8.

	BTC	ETH	XRP	ADA	MATIC	LTC	LINK
BTC	1,0000	0,8162	0,5708	0,6628	0,5895	0,8048	0,6681
ETH	0,8162	1,0000	0,6031	0,7159	0,6467	0,8223	0,7593
XRP	0,5708	0,6031	1,0000	0,5636	0,5014	0,6496	0,5685
ADA	0,6628	0,7159	0,5636	1,0000	0,6138	0,7033	0,6788
MATIC	0,5895	0,6467	0,5014	0,6138	1,0000	0,6076	0,6141
LTC	0,8048	0,8223	0,6496	0,7033	0,6076	1,0000	0,7256
LINK	0,6681	0,7593	0,5685	0,6788	0,6141	0,7256	1,0000

Tabela 3: Matriz de correlação entre os ativos. Elaboração própria.

A segunda matriz a ser elaborada é a da covariância, uma matriz quadrada que possui as variâncias e covariâncias associadas a cada ativo entre si (ex.: o quanto o Bitcoin varia dado a variação do Litecoin). O objetivo da mesma no presente estudo é encontrar possíveis combinações de carteiras ideais, visto que para encontrar uma carteira que gere um retorno esperado máximo (Max R(e)), usa-se de variações de preços também máximos.

	BTC	ETH	XRP	ADA	MATIC	LTC	LINK
BTC	0,0015	0,0016	0,0014	0,0015	0,0018	0,0016	0,0017
ETH	0,0016	0,0026	0,0020	0,0022	0,0026	0,0022	0,0025
XRP	0,0014	0,0020	0,0041	0,0022	0,0026	0,0022	0,0024
ADA	0,0015	0,0022	0,0022	0,0036	0,0030	0,0022	0,0026
MATIC	0,0018	0,0026	0,0026	0,0030	0,0065	0,0026	0,0032
LTC	0,0016	0,0022	0,0022	0,0022	0,0026	0,0028	0,0025
LINK	0,0017	0,0025	0,0024	0,0026	0,0032	0,0025	0,0042

Tabela 4: Matriz de covariância entre os ativos. Elaboração própria.

5.3 CARTEIRAS

A primeira carteira a ser encontrada é a que combina pesos iguais entre os ativos (*Equally-Weighted Portfolio*), e visto que são sete ativos observados, têm-se 14,29% alocado para cada ativo. Dado os retornos diários esperados E(r) da Tabela 2, encontrou-se, por meio de (1), o Retorno Esperado $R(e) = 0{,}36\%$ ao dia ou $265{,}51\%$ ao ano. Quanto a sua variação, esta foi encontrada por meio de (2), em modo matricial, no valor de 0,24%. Seu desvio padrão, que é a raiz da variação, foi de 4,91% e o Índice de Sharpe, encontrado por (3) foi de 0,0702.

A segunda carteira a ser encontrada é a que objetiva ter a menor variação possível (*Min Variance Weights*), dados os pesos e retornos disponíveis. Encontrou-se um retorno diário esperado de 0,18% ao dia ou 91,97% ao ano, uma variação de 0,15%, desvio padrão de 3,83%, Índice de Sharpe de 0,0438 e pesos de 97,91% para Bitcoin, 2,09% para Ripple e 0,00% para os demais.

A terceira carteira é a que maximiza o Índice de Sharpe (*Optimal Risky Portfolio*), gerando a carteira com melhor combinação entre o risco e o retorno esperado. Gerando os resultados de 0,57% ao dia de retorno esperado ou 701,18% ao ano, variação de 0,39%, desvio padrão de 6,27% e Índice de Sharpe de 0,0894; por meio dos pesos: 25,21% para Ethereum, 17,92% para Cardano, 56,87% para Polygon e 0,00% para os demais.

A quarta carteira, maximiza o retorno esperado (*Max Expected Return*). Dessa forma, encontrou-se que 100% da carteira ficaria alocada em Polygon, gerando 0,71% de retorno esperado diário ou 1212,84% ao ano, variação de 0,65%, desvio padrão de 8,06% e Índice de Sharpe de 0,0864.

De maneira resumida:

Carteira	Pesos	R(e)	σp²	σp	Sharpe
Pesos Iguais	14,29% para todos	0,36%	0,24%	4,91%	0,0702
Variação Mínima	97,91% (BTC) e 2,09% (XRP)	0,18%	0,15%	3,83%	0,0438
Eficiente	25,21% (ETH), 56,87% (MATIC) e 17,92% (ADA)	0,57%	0,39%	6,27%	0,0894
Retorno Esperado Máximo	100% (MATIC)	0,71%	0,65%	8,06%	0,0864

Tabela 5: Carteiras encontradas. Elaboração própria.

Por fim, para demonstrar a fronteira eficiente de Markowitz, gerou-se uma base de dados aleatória com 150 mil pesos, retornos e desvios-padrão diferentes. Com isso, tem-se a

Figura 5, que possibilita ver as carteiras geradas de maneira aleatória (rw), a carteira com variação mínima (mv), a eficiente (ef) e a com pesos iguais (ew). Com a carteira eficiente sendo tangenciada pela *Capital Allocation Line* (CAL).

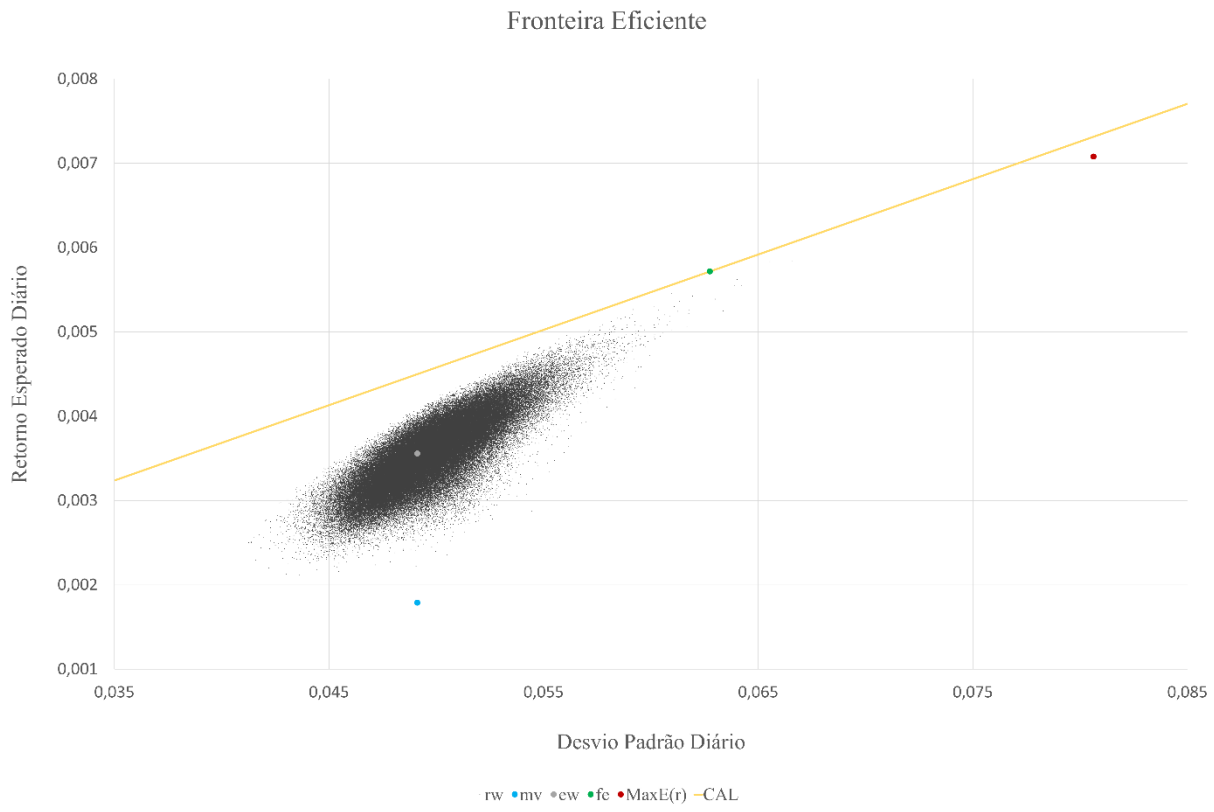


FIG. 5: Fronteira Eficiente de Markowitz dos ativos. Elaboração própria.

Com a Figura 5, pode-se deduzir algumas informações quanto a escolha dos ativos: (i) apesar da escolha ter sido aleatória, por serem criptoativos, possuem uma correlação próxima entre si; (ii) os criptoativos possuem uma variação de preços incomum, sendo que, para gerar um retorno esperado máximo, é preciso escolher um ativo "novo", e aproveitar sua escalada de preços (ex.: MATIC, que saltou de U$ 0,017 em 01/01/2020 para U$ 2,877 em 26/12/2021, gerando mais de 19 mil pontos percentuais de retorno); (iii) os ativos possuem maior correlação com o Bitcoin, como se a mesma fosse uma empresa líder de mercado que define o preço e as demais tem de a acompanhar, desta forma, para uma variação de carteira mínima é preciso manter maior parte do capital alocado em Bitcoin.

Quanto as volatilidades, constatou-se que os criptoativos possuem uma ascendência e queda que pode passar de 16 mil pontos percentuais. Sendo o nível de volatilidade adotado o

fator fundamental ao retorno esperado, como pode ser visto na Figura 6, as carteiras encontradas mostraram que quanto maior o apetite ao risco, maior deverá, necessariamente, ser o retorno esperado exigido. Entretanto, não necessariamente o maior retorno exigido deverá ser uma carteira diversificada, visto que o encontrado no modelo estudado retornou o ativo MATIC com peso máximo na carteira, e a carteira que maximiza o desvio padrão utilizou apenas três dos sete ativos disponíveis.

FIG. 6: Retorno acumulado das carteiras. Elaboração própria.

6 CONCLUSÃO

O estudo da criação de um portifólio de criptoativos se demonstrou satisfatório, trazendo resultados quanto a relação dos criptoativos entre si. Foi possível observar que em todas as carteiras criadas, de maneira aleatória e sem vieses, o retorno esperado anual se mostrou superior ao ativo livre de risco e, quando comparado ao retorno acumulado anual dos maiores fundos multimercado de 2021 (Tabela 1), todas as carteiras (exceto a com variância mínima) superam tais fundos. Demonstrando que a possibilidade do uso de uma carteira com criptoativos é plausível ao investimento, bastando apenas que o investidor tenha apetite ao risco.

Por meio das Tabelas 3 e 4 foi possível visualizar a correlação e covariância dos ativos escolhidos, respectivamente. Com as mesmas constatou-se que os criptoativos possuem uma proximidade considerável entre si, visto que, de -1 a 1, todas as relações de correlação entre eles foram superiores a 0,5. E a matriz de covariância se mostrou numa faixa de 0,0014 (BTC, XRP) a 0,0065 (MATIC, MATIC).

Foi possível observar a Fronteira Eficiente de Markowitz por meio da Figura 5 e analisar a volatilidade por meio da Figura 6. Ambas demonstrando que quanto maior o risco para o investimento, maior deverá ser o retorno exigido pelo investidor.

Com base nos resultados obtidos, o presente estudo espera servir como uma base para que investidores avessos a esta tecnologia, seja por quaisquer motivos forem, venham a conhecê-la e entender a sua aplicação em uma carteira maximizada. Visto que, como é uma novidade monetária e de pagamentos disruptiva, é compreensível a aversão ao novo, ainda mais quando essa tecnologia é usada por alguns indivíduos para cometer crimes. Crimes estes que seriam facilmente evitáveis se o investidor conhecesse os mecanismos criptográficos, não necessariamente de forma aprofundada, que possibilitam o funcionamento da ferramenta.

Quanto a fazer uso de criptoativos como uma forma de investimento, é preciso ir além deste estudo, visto que por detrás de cada criptoativo há uma equipe ou comunidade que gera (ou não) valor/lastro para o mesmo. Sendo necessário fazer uma análise fundamentalista do projeto como um todo e não somente se basear nos preços passados.

Há também a possibilidade de novos estudos que venham a preencher lacunas que este trabalho não veio a propor solucionar, como é o caso do estudo dos criptoativos com a metodologia *Value at Risk* (VaR), a análise dos mesmos para diferentes períodos (como antes e depois da pandemia do COVID-19 ou para períodos de alta e baixa de preços) e para a comparação com outros benchmarks. Ou seja, há ainda a possibilidade de muitos estudos sobre o tema, visto que não somente a tecnologia é recente, como também suas análises.

7 REFERÊNCIAS

ARRAEZ, J.; VALDERRAMA, S. **Venezuelanos não sentem no bolso o fim da hiperinflação**. Caracas: Valor Econômico, 2022. Disponível em: <https://valor.globo.com/mundo/noticia/2022/01/22/venezuelanos-nao-sentem-no-bolso-o-fim-da-hiperinflacao.ghtml>. Acesso em: 08 de dez. de 2022.

ATKINS, D; STALLINGS, W; ZIMMERMANN, P. **PGP Message Exchange Formats**. RFC 1991, 1991. Disponível em: <https://www.rfc-editor.org/rfc/rfc1991>. Acesso em: 06 de out. de 2022.

BACK, A. **Hash cash postage implementation**. 1997. Disponível em: <http://www.hashcash.org/papers/announce.txt>. Acesso em: 06 de out. de 2022.

BACK, A. **Hashcash:** A Denial of Service Counter-Measure. 2002. Disponível em: <http://www.hashcash.org/papers/hashcash.pdf>. Acesso em: 06 de out. de 2022.

BALL, M; KLUGER, J; DE LA GARZA, A. **2021 Person of the Year:** Elon Musk. Revista Time, Califórnia, 13 de dez. de 2021. Disponível em: <https://time.com/person-of-the-year-2021-elon-musk/>. Acesso em: 14 de dez. de 2021.

BAYER, D.; HABER, S.; STORNETTA, W.S. **Improving the Efficiency and Reliability of Digital Time-Stamping**. Sequences II. Springer, New York, 1993. Disponível em: <https://doi.org/10.1007/978-1-4613-9323-8_24>. Acesso em: 06 de out. de 2022.

BERK, J.; DEMARZO, P. **Finanças Empresariais**. Porto Alegre: Bookman, 2009.

BRASIL. **Calculadora Cidadão**. Banco Central do Brasil, 2022.

BRASIL. **Parecer de Orientação CVM nº 40, de 11 de outubro de 2022**. Dispõe sobre os CriptoAtivos e o Mercado de Valores Mobiliários. Comissão de Valores Mobiliários, 2022. Disponível em: <https://conteudo.cvm.gov.br/legislacao/pareceres-orientacao/pare040.html>. Acesso em: 08 de dez. de 2022.

BRASIL. Câmara dos Deputados. **PL 4401/2021** (Nº Anterior: PL 2303/2015). Distrito Federal, 2021.

CERF, V; KAHN, R. **A Protocol for Packet Network Intercommunication**. IEEE Transactions on Communications, vol. 22, no. 5, pp. 637-648, maio de 1974. Disponível em: <https://ieeexplore.ieee.org/document/1092259>. Acesso em: 30 de set. de 2022.

CFI. **Capital Allocation Line (CAL) and Optimal Portfolio**. Corporate Finance Institute, 2022. Disponível em: <https://corporatefinanceinstitute.com/resources/wealth-management/capital-allocation-line-cal-and-optimal-portfolio/>. Acesso em: 01 de nov. de 2022.

CHAINALYSIS. **The 2022 Global Crypto Adoption Index:** Emerging Markets Lead in Grassroots Adoption, China Remains Active Despite Ban, and Crypto Fundamentals Appear Healthy. Chainalysis, 2022. Disponível em: <https://blog.chainalysis.com/reports/2022-global-crypto-adoption-index/>. Acesso em: 08 de out. de 2022.

CHAUM, D. **Blind Signatures for Untraceable Payments**. Advances in Cryptology, pp. 199–203, 1983. Springer, Boston, MA. Disponível em: <https://doi.org/10.1007/978-1-4757-0602-4_18>. Acesso em: 30 de set. de 2022.

CHAUM, D. **Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms**. Communications of the ACM, vol. 24 n. 2, fev. 1981 pp 84–90 Disponível em: <https://doi.org/10.1145/358549.358563>. Acesso em: 01 de out. de 2022.

CHEN, J. **Liberty Reserve**. Investopedia, 2020. Disponível em: <https://www.investopedia.com/terms/l/liberty-reserve.asp>. Acesso em: 07 de out. de 2022.

COINBASE. **What is a seed phrase?** Coinbase, 2021. Disponível em: <https://www.coinbase.com/pt/learn/crypto-basics/what-is-a-seed-phrase>. Acesso em: 12 jan. 2022.

CORACCINIL, R; **Tesla passa a aceitar bitcoins na compra de carros nos Estados Unidos**. CNN Brasil, 24 de mar. 2021. Disponível em: <https://www.cnnbrasil.com.br/business/tesla-passa-a-aceitar-bitcoins-na-compra-de-carros-nos-estados-unidos/>. Acesso em: 14 de dez. de 2021.

CRIPTO, E. **Os predecessores do Bitcoin**. Money Times, 2021. Disponível em: <https://www.moneytimes.com.br/escolacripto-os-predecessores-do-bitcoin/#:~:text=DigiCash,an%C3%B4nimo%20que%20usou%20protocolos%20criptogr%C3%A1ficos>. Acesso em: 27 de jul. de 2022.

DIFFIE, W; HELLMAN, M. **New Directions in Cryptography**. IEEE Transactions on Communications, vol. 22, no. 6, pp. 644-654, nov. de 1976. Disponível em: < https://ieeexplore.ieee.org/document/1055638 >. Acesso em: 30 de set. de 2022.

FINNEY, H. **RPOW:** Reusable Proofs of Work. 15 de ago. de 2004. Disponível em: <https://nakamotoinstitute.org/rpow/>. Acesso em: 06 de out. de 2022.

FISCHER, M; LYNCH, N; PATERSON, M. **Impossibility of distributed consensus with one faulty process**. Journal of the ACM, vol. 32, n. 2, 1985. Disponível em: <https://doi.org/10.1145/3149.214121>. Acesso em: 01 de out. de 2022.

GRIGG, I. **The Ricardian Contract**. Proceedings. First IEEE International Workshop on Electronic Contracting, 2004. pp. 25-31. Disponível em: <https://doi.org/10.1109/WEC.2004.1319505>. Acesso em: 07 de out. de 2022.

HABER, S.; STORNETTA, W.S. **How to time-stamp a digital document**. J. Cryptology 3, 99–111 (1991). Disponível em: <https://doi.org/10.1007/BF00196791>. Acesso em: 06 de out. de 2022.

HAYEK, F.A. **Desestatização do Dinheiro**. 2 ed. São Paulo: Instituto Ludwig von Mises Brasil, 2011.

HERINGER, S; SOUZA, R. **'Faraó dos Bitcoins':** Conheça a saga do ex-garçom que chegou a movimentar R$ 38 bilhões. Rio de Janeiro: O Globo Rio, 05 de set. de 2021. Disponível em: <https://oglobo.globo.com/rio/farao-dos-bitcoins-conheca-saga-do-ex-garcom-que-chegou-movimentar-38-bilhoes-25180007>. Acesso em: 08 de out. de 2022.

HONG, K. H. (2017). **Bitcoin as an alternative investment vehicle**. Information Technology and Management, 18(4), 265-275. Disponível em: <https://doi.org/10.1007/s10799-016-0264-6>. Acesso em: 12 de jan. de 2022.

HUGHES, E. **A Cypherpunk's Manifesto**. Activism, 9 de mar. de 1993. Disponível em: <https://www.activism.net/cypherpunk/manifesto.html>. Acesso em: 08 de out. de 2022.

HÜLSMANN, J. **The Ethics of Money Production**. Alabama: Mises Institute, 2008.

INVESTING. **BTC/BRL**: Bitcoin Real Brasileiro. Investing, 2022. Disponível em: <https://br.investing.com/crypto/bitcoin/btc-brl-historical-data>. Acesso em: 12 de jan. de 2022.

KANSAL, S. **Merkle Trees:** What They Are and the Problems They Solve. Codementor, 2020. Disponível em: <https://www.codementor.io/blog/merkle-trees-5h9arzd3n8>. Acesso em: 30 de set. de 2022.

LI, J-P.; NAQVI, B.; RIZVI, S. K.; CHANG, H-L. **Bitcoin:** The biggest financial innovation of fourth industrial revolution and a portfolio's efficiency booster. Elsevier, 2021. Disponível em: <https://doi.org/10.1016/j.techfore.2020.120383>. Acesso em: 17 nov. 2021.

LI, Y. **Charlie Munger calls bitcoin 'disgusting and contrary to the interests of civilization'**. CNBC, 1 de maio de 2021. Disponível em: <https://www.cnbc.com/2021/05/01/charlie-munger-calls-bitcoin-disgusting-and-contrary-to-the-interests-of-civilization.html>. Acesso em: 14 de dez. de 2021.

MAHONEY, D. **A Teoria Austríaca dos Ciclos Econômicos:** Uma Breve Explanação. Instituto Ludwig von Mises Brasil, 2008. Disponível em: <https://www.mises.org.br/article/141/a-teoria-austriaca-dos-ciclos-economicos-uma-breve-explanacao>. Acesso em 08 de dez. de 2022.

MARKOWITZ, H. **Portfolio Selection**. The Journal of Finance, v. 7, n. 60, p. 77–91, 1952. Disponível em: <https://doi.org/10.2307/2975974>. Acesso em: 12 de jan. 2022.

MATOS, G. **Saiba o que foi o Pizza Day do Bitcoin**. Criptofácil, 22 de maio de 2020. Disponível em: <https://www.criptofacil.com/voce-conhece-o-bitcoin-pizza-day/>. Acesso em: 12 de jan. de 2022.

MAY, T. **The Crypto Anarchist Manifesto**. Nakamoto Institute, 1988. Disponível em: <https://nakamotoinstitute.org/crypto-anarchist-manifesto/>. Acesso em: 08 de out. de 2022.

NAKAMOTO, S. **Bitcoin:** A Peer-to-Peer Electronic Cash System, 2008. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 14 de dez. de 2021.

PLANB. **Modeling Bitcoin Value with Scarcity**. Medium, 2019. Disponível em: <https://medium.com/@100trillionUSD/modeling-bitcoins-value-with-scarcity-91fa0fc03e25>. Acesso em: 12 de jan. de 2022.

REIFF, N. **What Was the First Cryptocurrency?** Investopedia, 23 de jul. 2022. Disponível em: <https://www.investopedia.com/tech/were-there-cryptocurrencies-bitcoin/>. Acesso em: 27 de set. de 2022.

ROCHA, L. **Divisor de águas: veja as principais opiniões do mercado sobre a regulamentação de criptomoedas no Brasil**. Criptofácil, 2022. Disponível em: <https://www.criptofacil.com/divisor-de-aguas-veja-as-principais-opinioes-do-mercado-sobre-a-regulamentacao-de-criptomoedas-no-brasil/>. Acesso em: 08 de dez. de 2022.

ROTHBARD, Murray N. **A ética da liberdade**. 2 ed. São Paulo: Instituto Ludwig von Mises Brasil, 2010.

ROTHBARD, Murray N. **O que o governo fez com o nosso dinheiro?** 1 ed. São Paulo: Instituto Ludwig von Mises Brasil, 2013.

SCHELLINGER, B. **Optimization of special cryptocurrency portfolios**. Journal of Risk Finance, Vol. 21 No. 2, pp. 127-157. Disponível em: <https://doi.org/10.1108/JRF-11-2019-0221>. Acesso em: 17 nov. 2021.

SHARMA, R. **Bit Gold**. Investopedia, 2021. Disponível em: <https://www.investopedia.com/terms/b/bit-gold.asp>. Acesso em: 06 de out. de 2022.

SIDHU, R. **Exploring Bitcoin's History:** It took 40 years of discoveries and inventions for BTC to become a reality. Medium, 2021. Disponível em: < https://medium.com/coinmonks/exploring-bitcoins-history-ecbf1c59952c >. Acesso em: 30 de set. de 2022.

SILVA, S. C.; MONTEIRO, V. B. **Criptomoedas (ou criptoativos?) como meio de pagamento no Brasil e a lógica do Cisne Negro:** da ausência de regulamentação específica ao desempenho da criptoeconomia durante a pandemia de Covid-19. EALR: Brasília, v.12, n.2, p. 145-170, mai/ago, 2021.

SZABO, N. **Formalizing and Securing Relationships on Public Networks**. First Monday, 2, no. 9, 19h97. Disponível em: <http://firstmonday.org/ojs/index.php/fm/article/view/548/469>. Acesso em: 06 de out. de 2022.

SZABO, N. **Secure Property Titles with Owner Authority**. 1998. Disponível em: <https://nakamotoinstitute.org/literature/secure-property-titles/>. Acesso em: 06 de out. de 2022.

TOLOTTI, R. **Bitcoin em queda:** o que esperar após a desvalorização de mais de 20% no final de semana? Infomoney, 6 de dez. de 2021. Disponível em: <https://www.infomoney.com.br/mercados/bitcoin-em-queda-o-que-esperar-apos-a-desvalorizacao-de-mais-de-20-no-final-de-semana/>. Acesso em: 14 de dez. de 2021.

VASCONCELOS, G. **Regulamentação de criptos deve ser feita de maneira pouco invasiva, aponta CVM**. eInvestidor, 2022. Disponível em: <https://einvestidor.estadao.com.br/ultimas/cvm-regulamentacao-criptomoedas-pouco-invasiva/>. Acesso em: 08 de dez. de 2022.

VELLEDA, I. **Como funciona a mineração de bitcoins?** Forbes, 8 de dez. de 2021. Disponível em: <https://forbes.com.br/forbes-money/2021/12/como-funciona-a-mineracao-de-bitcoins/>. Acesso em: 12 de jan. de 2022.