

INSTITUTO DE MATEMÁTICA E ESTATÍSTICA
CURSO DE GRADUAÇÃO
DE LICENCIATURA EM MATEMÁTICA

LUCAS HERICK PEREIRA DA SILVA

*DO LEGADO AOS CRIPTOATIVOS:
UMA PERSPECTIVA DOS MEIOS DE
PAGAMENTO PARA O ENSINO BÁSICO*

UNIVERSIDADE
FEDERAL
FLUMINENSE



NITERÓI
2022

LUCAS HERICK PEREIRA DA SILVA

DO LEGADO AOS CRIPTOATIVOS: UMA PERSPECTIVA DOS MEIOS DE
PAGAMENTO PARA O ENSINO BÁSICO

Trabalho de Conclusão de Curso
apresentada à Coordenação do Curso
Graduação de Licenciatura em Matemática
da Universidade Federal Fluminense
como requisito parcial para aprovação na
disciplina Trabalho de Conclusão de Curso
II (GTL00003).

Orientador: Prof. Dr. Mohammad Fanaee

Niterói-RJ
2022

Ficha catalográfica automática - SDC/BIME
Gerada com informações fornecidas pelo autor

S5861 Silva, Lucas Herick Pereira da
DO LEGADO AOS CRIPTOATIVOS: UMA PERSPECTIVA DOS MEIOS DE
PAGAMENTO PARA O ENSINO BÁSICO / Lucas Herick Pereira da Silva
; Mohammad Fanaee, orientador. Niterói, 2022.
77 p. : il.

Trabalho de Conclusão de Curso (Graduação em Matemática)-
Universidade Federal Fluminense, Instituto de Matemática e
Estatística, Niterói, 2022.

1. Transferência eletrônica de fundos. 2. Criptografia. 3.
Moeda estrangeira. 4. Mineração de dados (Computação). 5.
Produção intelectual. I. Fanaee, Mohammad, orientador. II.
Universidade Federal Fluminense. Instituto de Matemática e
Estatística. III. Título.

CDD -

LUCAS HERICK PEREIRA DA SILVA

DO LEGADO AOS CRIPTOATIVOS: UMA PERSPECTIVA DOS MEIOS DE
PAGAMENTO PARA O ENSINO BÁSICO

Trabalho de Conclusão de Curso apresentada à Coordenação do Curso Graduação de Licenciatura em Matemática da Universidade Federal Fluminense como requisito parcial para aprovação na disciplina Trabalho de Conclusão de Curso II (GTL00003).

Aprovada em 28/*Jan*/2022

Banca Examinadora

Prof. Mohammad Fanaee - Orientador
D.Sc - Universidade Federal Fluminense

Prof. Anderson Mayrink da Cunha - Membro
D.Sc - Universidade Federal Fluminense

Prof. Vahid Nikoofard - Membro
D.Sc - Universidade Estadual do Rio de Janeiro

*Esta obra é integralmente dedicada aos meus amados pais, digníssimos Sra. Francisca e Sr. Jozivan Pereira.
Minha base forte e exemplos de autarquia.*

Agradecimentos

Ao único e poderoso Deus, que me deu a oportunidade de chegar até aqui, dando-me propósito, perdoando minhas falhas, guiando-me, preservando minha fé, que deu-me uma formação espiritual suficientemente forjada para perseverar e prevalecer contra os pecados e tentações tão amplamente disponíveis no ambiente universitário. Deus não está morto, certamente vivo está!

Ao meu núcleo familiar, meus amados pais, digníssimos Sra. Francisca e Sr. Jozivan Pereira. Estes foram responsáveis por serem exemplos de rigor, sabedoria, integridade e carinho para minha formação, governando-me no caminho que devo andar, em disciplina e admoestação, provendo sabedoria nos momentos de adversidade, ensinando-me sobre as santas escrituras e disciplinando quando necessário. Esta conquista é vossa e também todas as outras que ainda hão de surgir ♡

A minha amada irmã Sra. Francine Oliveira, que me fez relembrar que a matemática não está limitada somente ao escopo da docência, mas sendo também a base do mundo corporativo. Agradeço por seus ensinamentos dentro da Engenharia e Análise de Dados, *Business Intelligence* e sistemas Linux. Estes me fizeram desenvolver interesse nas mais diversas *libraries(Libs)*, e estruturas de programação como *Structured Query Language (SQL)* e *Python/Python Spark PySpark*.

Aos meus queridos tios, Sra. Marcia e Sr. Jary Amorim, que por sua intervenção me permitiram prosseguir com os estudos.

Aos professores, em especial aqueles que possibilitaram escrever parte da minha história dentro do instituto de matemática e estatística da universidade federal fluminense. São eles: Fábio Henrique e Roberto Geraldo do departamento de geometria, Ricardo Apolaya, Renata de Freitas, Miriam Abdon, Anne Michelle e Paulo Trales do departamento de análise, Carlos Mathias, Humberto Bortolossi e Sebastião Firmino (in memoriam) do departamento de matemática aplicada. Mestres, dou-lhes minha admiração e respeito, saúdo-vos

e agradeço-vos pela maestria em suas atuações.

Ao professores Fabiano Souza e Sandra William, que foram meu mentores na primeira seleção do Programa Institucional de Residência Pedagógica. Com vossas permissões consegui desenvolver e aplicar diversos projetos tecnológicos para muitos alunos das mais diversas turmas de matemática, projetos que variam de aplicações em simuladores de voo até protótipos de aplicativos android compilados em C# e Unity.

Ao meu orientador Prof Dr. Mohammad Fanaee por me receber como orientado em seu gabinete. Agradeço imensamente pela confiança no meu trabalho, pela compreensão, pelo respeito, por seus excelentes ensinamentos não só de matemática mas de vivência por meio de sábios conselhos em vários momentos da graduação.

A esta pequena lista dos mais memoráveis camaradas da jornada universitária: Alexandre Lopes, Everaldo Costa, Lair Júnior, Leandro Goiano, Janaína Citeli, Jéssica Cecília da química, Matheus Gama, Nayara Lima, Renan Santo, Raphael Odalvo, Victor Chirity e Victor Sarmet. Agradeço pelas tardes e noites viradas de estudo, pelos almoços e jantares no restaurante universitário, idas e vindas nas bibliotecas da universidade e pelas incontáveis vezes no qual a vida se tornou mais significativa com vós. Camaradas, permaneци firmes, pois as provações são grandes, mas a vitória (a formatura!) é iminente.

Finalmente, meu agradecimento a todos aqueles que não tiveram menção direta mas tive o prazer de conhecer, que pude ajudar, que recebi alguma ajuda e acompanhei direta ou indiretamente, expandindo meu networking acadêmico e profissional.

Obrigado. Thank you. Merci. Gracias. 감사합니다 (gamsahamnida).

“I know what it’s like to be afraid of your own mind.”

Dr. Spencer Reid ¹

¹ Eu sei o que é ter medo de sua própria mente. (Tradução livre). Criminal Minds.

RESUMO

O propósito do presente instrumento é disseminar a criptoliteracia que é o conhecimento sobre criptomoedas, argumentando sobre suas funções e características com uma abordagem simplificada e compreensão desembaraçada. Assim, a história das transações humanas é resumida em um breve contexto histórico, é feita uma introdução aos principais conceitos da criptografia que é a base do sistema, e uma ideia geral sobre o que são criptomoedas e uma percepção geral da população mundial sobre o tema é exibido. Além disso, uma proposta de atividade é totalmente desenvolvida. A atividade busca mostrar de forma prática os ganhos e perdas na mineração de criptomoedas por meio do cálculo do tempo de retorno adequado do investimento em hardware on-premise, tudo como resultado de grandezas de potência computacional em conversão de gasto de energia e conceitos primários de matemática financeira e elementar. O autor espera que um dia, em um futuro próximo, os investimentos em criptoativos sejam uma opção mais acessível, simples de aplicar e compreender para quem tem vontade de investir, independente de renda, condição social, escolaridade e sexo.

Palavras-chave: Criptomoedas; Meios de Pagamento; Criptografia; Mineração.

ABSTRACT

The purpose of this instrument is to disseminate cryptoliteracy, which is the knowledge about cryptocurrencies, arguing about its functions and characteristics with a simplified approach and disentangled understanding. Accordingly, the history of human transactions is summarized in a brief historical context, an introduction to the main concepts of cryptography which is the system basis is done, and a general idea about what cryptocurrencies are and a general perception of the world population about the topic is displayed. Furthermore, an activity proposal is fully developed. The activity seeks to show in a practical way the gains and losses in cryptocurrency mining through calculating the payback time appropriate on-premise hardware investment, all as a result of computational power quantities into energy expenditure conversion and primary concepts of financial and elementary mathematics. The author hopes that one day, in the near future, investments in cryptoactives will be a more accessible option, simple to apply and comprehend for those who have the desire to invest, regardless of income, social status, educational status and sex.

Keywords: Cryptocurrencies; Payment methods; Cryptography; Cryptocurrencies Mining.

SUMÁRIO

1	INTRODUÇÃO	17
1.1	Contextualização	17
1.2	Temática	18
1.3	Objetivos	18
1.3.1	Objetivo Geral	18
1.3.2	Objetivos Específicos	19
1.4	Estruturação do trabalho	19
1.5	Relevância do estudo	20
2	UMA SÍNTESE DAS TRANSAÇÕES: DA PRÉ-HISTÓRIA AOS SISTEMAS DIGITAIS	21
2.1	Prólogo	21
2.2	O princípio	22
2.2.1	Escambo	22
2.2.2	Conchas (e outros objetos)	23
2.3	A jornada dos metais	24
2.3.1	Cunhagem	25
2.3.2	A primeira moeda oficial	26
2.4	A transição para o papel moeda	27
2.5	Guerras cambiais	28
2.6	Uma nova era: Cartões e ATMs	29
2.7	Transações eletrônicas: dinheiro e bancos digitais	30
3	O FUTURO: CRIPTO	32
3.1	Uma noção rápida sobre criptografia	32
3.1.1	Idéia geral	32
3.1.2	Métodos criptográficos históricos	33
3.1.3	Chaves criptográficas	34
3.1.4	A tecnologia blockchain	35

3.2	Os criptoativos	36
3.2.1	Conceito	36
3.2.2	Concepção	36
3.2.3	Receptividade no mundo e na sociedade brasileira	37
3.2.3.1	No mundo	37
3.2.3.2	No Brasil	37
3.2.4	Proposta de modelo de pesquisa (com questionário)	38
3.2.4.1	Resolução do teste rápido apresentado	38
4	PROPOSTA DE ATIVIDADE E <i>HANDS ON!</i>	42
4.1	Introdução	42
4.1.1	Motivador para a atividade	43
4.2	Embasamento da atividade	43
4.2.1	Bases necessárias para a atividade	43
4.2.1.1	Matemática Financeira	44
4.2.1.2	Conversões de medidas	44
4.2.2	Embasamento de construção	45
4.2.2.1	Acadêmico	45
4.2.3	Infraestruturas digitais	46
4.2.3.1	On premise versus cloud	46
4.2.3.2	Sistemas operacionais	47
4.3	Guia para o professor e guia para o <i>Hands on!</i>	47
4.3.1	Orientações gerais para uso da planilha piloto	49
4.4	Exemplo de plano de aula	51
4.4.1	Materiais necessários e opcionais	52
4.4.2	Metodologia	52
4.4.3	Avaliação	53
4.5	Exemplo de resultado	54
5	CONSIDERAÇÕES FINAIS	56
5.1	Conclusões	56
5.2	Trabalhos futuros	57
Referências Bibliográficas		58
Apêndice		62
Glossário		73

Lista de ilustrações

Figura 1 – Escambo: Um acordo entre duas partes	23
Figura 2 – Introdução ao dinheiro	24
Figura 3 – O “Leão Lidiano”, a primeira moeda	26
Figura 4 – Mapa da Lídia de 1903	27
Figura 5 – Cartas assinadas	28
Figura 6 – Exemplos de moedas fiduciárias atuais	29
Figura 7 – Resumo do capítulo em uma imagem	31
Figura 8 – Medalhão de cifra de César disponível para venda	34
Figura 9 – Esquema de funcionamento das criptografias por chave pública e por chave privada	35
Figura 10 – Um passeio veicular com Dogecoin e Ethereum	43
Figura 11 – Arquitetura de um RIG	47
Figura 12 – Guia de cores dos botões de seleção de GPUs	48
Figura 13 – Outras opções da calculadoras	48
Figura 14 – Exemplos de diferentes algorítmos de mineração disponíveis nas calcu- ladoras	49
Figura 15 – Lista de lucratividade média diária de criptomoedas	53
Figura 16 – Planilha de cálculo de lucros, parte 1	54
Figura 17 – Planilha de cálculo de lucros, parte 2	54

Lista de tabelas

Tabela 1 – Objetivos gerais da criptografia	33
Tabela 2 – Tipos de chaves criptográficas	35
Tabela 3 – Tabela de conversão de hashes	45
Tabela 4 – Tabela de conversão de armazenamento computacional	45
Tabela 5 – Exemplo de plano de aula	51

Lista de abreviaturas e siglas

ATM	Automated Teller Machine ou caixa eletrônico
BNCC	Base Nacional Comum Curricular
BRL	Brazilian Real ou Real Brasileiro. Moeda nacional Brasileira
BTC	Criptomoeda Bitcoin
CDBC	Central Bank Digital Currency ou moeda digital emitida por banco central
DOC	Documento de Crédito
EB	Ensino básico ou Ensino Fundamental
EF	Educação financeira
EFT	Eletronic Fund Transfers ou transferências de fundos eletrônicos
EM	Ensino médio
ETH	Criptomoeda Ethereum
FIRO	Criptomoeda antes conhecida por Zcoin
GB	Gigabyte
GPU	<i>Graphic Processing Unit</i> ou Unidade
<i>h/s</i>	Hashes por segundo, ou Hashrate
IoT	<i>Internet of Things</i> ou Internet das coisas
LIBs	<i>Libraries</i> ou bibliotecas
ML	<i>Machine Learning</i> ou aprendizado de máquina
NFT	Non-fungible Token ou Token não fungível

PL	Projeto de lei
RAM	<i>Random Access Memory</i> ou Memória de acesso randômico
RVN	Criptomoeda Ravencoin
SHA-2	<i>Secure Hash Algorithm 2</i> ou Algorítmo de hash seguro 2
SI	Sistema Internacional de Unidades
SQL	<i>Structured Query Language</i> ou Linguagem de consulta estruturada
TCC	Trabalho de conclusão de curso
TED	Transferência Eletrônica Digital de processamento gráfico
USD	United States Dollar ou dólar americano. Moeda nacional dos Estados Unidos da América
VRAM	<i>Video Random Access Memory</i> ou Memória de acesso randômico de vídeo
WU	Banco Western Union

Capítulo 1

Introdução

“(O) Bitcoin fará aos bancos o que o e-mail fez à indústria postal” - Rick Falkvinge¹
(tradução livre)

Neste capítulo será feita uma breve introdução contextualizada, e falaremos sobre os objetivos e estruturas do documento.

1.1 Contextualização

A cada ano novas tecnologias tem tomado as prateleiras dos mercados de eletrodomésticos, eletroportáteis, a integração das tecnologias de *machine learning* (ML)² com inteligência artificial em *smart devices*³, que podemos citar como exemplo os assistentes pessoais, carros autônomos, a computação com *internet of things* (IoT)⁴. Seria evidente a criação de uma tecnologia ou moeda que reduzissem os trâmites em todas as relações financeiras que ocorrem diariamente em nossa sociedade.

¹ Citação original do inglês: “Bitcoin will do to banks what email did to the postal industry”

² Aprendizado de máquina, em tradução livre do inglês. Machine Learning trata do desenvolvimento e da utilização de sistemas computacionais que tenham a capacidade de aprender e se adaptar por conta própria, ou sejam, sem seguir instruções explícitas, por meio do treinamento de algoritmos e modelos estatísticos no intuito de obter inferências dentro de padrões em dados.

³ Aparelhos inteligentes, em tradução livre do inglês. Smart devices são dispositivos eletrônicos, que possuem conectividade com outros dispositivos pelos mais diferentes protocolos de conexão, como WiFi, Bluetooth, 3G, 4G, 5G, NFC, etc, que operando e possibilitando interações com os usuários e também de forma independente.

⁴ Internet das coisas, em tradução livre do inglês. São aparelhos que possuem a capacidade de transferir dados em uma rede sem a necessidade de interação homem para homem ou computador para homem. A definição de aparelhos inteligentes tem conexão direta com a internet das coisas.

O foco deste instrumento é baseado em criptoativos, uma tecnologia que tem alterado os padrões do mundo das finanças e já faz parte do mundo digital. Mas do que se tratam os criptoativos, as criptomoedas? Uma criptomoeda é uma moeda digital que pode ser usada para obtenção de bens e aquisição de serviços que baseia sua segurança em criptografia para proteger as transações online. Em sua variação de maior popularidade, o *Bitcoin (BTC)*, devido a sua especulação, tem enfrentado uma consequente volatilidade. Por exemplo, segundo dados do (COINBASE, 2021), em 11 de dezembro de 2020, 1 BTC valia R\$ 91.415,48, três meses depois, R\$ 321.078,18 e mais três depois voltou ao patamar de R\$ 191.042,90.

1.2 Temática

Caro leitor, tome o seguinte momento para questionar sobre o progresso tecnológico que ocorreu nos últimos anos. Pondere sobre como a tecnologia tem influenciado tua vida e daquele que lhe cercam e verás então como será importante o conhecimento sobre criptoativos nos dias futuros. Chris Garrod, em uma reportagem do site Conyers cita o seguinte:

Os mercados de criptomoedas estão em todos os lugares. (...) Não são ouro e nem dinheiro fiduciário⁵. Esta é uma tecnologia totalmente nova que já ilustrou sua capacidade de perturbar fundamentalmente o sistema financeiro global. (GARROD, 2018)

De fato, manter-se atualizado sobre o momento atual da tecnologia é fundamental. Considere a seguinte analogia: A moeda na era digital, se comparados aos meios de comunicação, é como ao e-mail versus o serviço físico postal. Antes da internet, as pessoas dependiam dos serviços postais para enviar uma mensagem a quem estivesse em outro lugar, era preciso um intermediário para entregá-la fisicamente, inimaginável para os possuidores do precursor da comunicação eletrônica e ainda mais inimaginável aos possuidores de seus sucessores, os serviços de mensageria criptografada. Isto é o que a criptomoeda se comparará ao dinheiro físico, perturbando fundamentalmente o sistema financeiro global, se observarmos a citação de (GARROD, 2018).

1.3 Objetivos

1.3.1 Objetivo Geral

Sintetizar a história das transações humanas em um breve contexto histórico e disseminar criptoliteracia que é o conhecimento sobre criptomoedas argumentando sobre

⁵ Veja mais sobre dinheiro fiduciário em 5

suas funções e características na esperança de em algum momento no futuro estes sejam acessíveis e de fácil compreensão, independentemente da renda, status educacional ou sexo.

1.3.2 Objetivos Específicos

- Desenvolver um breve histórico da evolução das transações humanas
- Introduzir sobre a história da criptografia e sobre como ela é a base das moedas virtuais.
- Trazer o conceito de criptoativo tomando nota de sua importância no cenário econômico atual.
- Propor uma atividade temática que mostre aos alunos os custos e lucros de se minerar criptoativos.

1.4 Estruturação do trabalho

O presente documento foi desenvolvido em quatro partes, permitindo assim que o prezado leitor tenha uma melhor separação de informações aqui prestadas e com isso uma melhor compreensão dos objetivos definidos no setor acima:

- No prólogo é apresentado uma introdução geral do tema, por meio de uma contextualização, juntamente com as definições tomadas.
- No segundo capítulo, é apresentado um resumo histórico das evoluções de transações e das moedas, como a utilização dos metais, evolução do papel moeda, cartões de débito e crédito até o dinheiro digital. Esta seção prepara o leitor para os criptoativos, tema do próximo capítulo.
- No terceiro capítulo, apresentaremos o futuro das moedas. Será feita uma introdução rápida sobre criptografia, uma ideia geral sobre o que são as criptomoedas e a percepção geral da população mundial sobre o tema. Esta seção prepara o leitor para a atividade do próximo capítulo.
- No quarto capítulo é desenvolvida uma atividade que mostre aos alunos o custos e ganhos na mineração de criptomoedas, além do cálculo do tempo de retorno do investimento de um hardware apropriado.

1.5 Relevância do estudo

A pesquisa pelo tema o que se apresenta neste presente documento se deu inicialmente na boa relação com o Prof Dr. Mohammad Fanaee. Em várias conversas durante os intervalos de suas aulas fui convidado a participar dos estudos orientados que ele também ministrava e palestras que ele participava. Uma destas palestras, ministrada pelo grupo Evolucionários da Universidade Federal Fluminense, cujo tema “Investimento de renda fixa e criptoativos” foi o marco inicial do interesse pelo tema. Nesse mesmo período, final de 2018, as moedas digitais já tinham um grande crescimento e conhecimento da mídia, principalmente o Bitcoin, que trouxe ao grupo de conversas diversos questionamentos sobre como estes aparatos tecnológicos poderiam impactar as economias tanto locais quanto internacionais. Apesar de sua alta volatilidade e serem definitivamente recentes, as criptomoedas já estão cada vez mais aparentes nos veículos de comunicação, com uma base de usuários crescente, com mais transações sendo realizadas diariamente, sem contar a vantagem de ser globalizada e ter como característica a descentralização sem fronteiras políticas e tendo ativo desenvolvimento.

Capítulo 2

Uma síntese das transações: da pré-história aos sistemas digitais

“Toda troca estimula a atividade produtiva, seja troca por presente, aposta, escambo ou transação com dinheiro.” - Aaron C. Brown¹.

(tradução livre)

Neste capítulo será apresentado um breve resumo histórico de como eram as realizadas as transações mostrando as bases do dinheiro que conhecemos hoje.

2.1 Prólogo

Ah, o dinheiro. Se o digníssimo leitor começasse a imaginar especificamente sobre este termo, muito provavelmente seus primeiros pensamentos seriam sobre todos os benefícios que este pode oferecer, digamos viagens para as mais belas paisagens disponíveis mundo afora, seja uma noite amena em um jantar requintado, um feriado em uma megalópole, além de muitas outras localidades. Alguns de nossos leitores também poderiam se encontrar imaginando notas de real, notas de euro, notas de dólar e moedas, outros ainda cartões de crédito e débito, vale refeição e alimentação. Arrisco ainda dizer que os ainda mais jovens pensariam na forma do dinheiro que se quer tocamos, que pode ser transferido digitalmente, com uso de ferramentas regulamentadas, como o PIX, por exemplo. O conceito de moeda

¹ Citação original do inglês: “All exchange stimulates productive activity, whether exchange by gift, gambling, barter, or money transaction.” em seu livro (BROWN, 2011)

^{2,3,4} que conhecemos hoje não é o mesmo de tempos remotos da passagem humana pelo planeta terra. Com efeito, se a pessoa mais rica do nosso país viajasse no tempo levando consigo sacolas com grande quantidade de dinheiro e se encontrasse com os humanos primitivos antes da era paleolítica, muitos deles veriam naquele montante somente alguma matéria prima para ser queimada e com isso obter uma fonte de calor para se proteger do frio. Tal diferença nas percepções de um mesmo objeto mostra o progresso da evolução humana, no qual neste tempo, este teve inúmeras alterações em sua estrutura no objetivo de satisfazer as necessidades sociais da população. Vejamos a seguir alguns momentos que foram fundamentais para esta evolução.

2.2 O princípio

2.2.1 Escambo

Em uma época onde não havia um objeto que por exemplo, se pudesse trocar uma saca de arroz por este que mais tarde seria trocado por outro produto, um galinha, por exemplo. Chamamos este objeto inexistente da época de moeda fiduciária (do inglês *Fiat Money*⁵) Nesta época as transações se baseavam em trocar bens por bens, bens por serviços ou serviços por serviços. Usando o exemplo que vimos anteriormente, há então duas possibilidades, se um criador de animais tivesse o desejo de se obter uma saca de arroz, este deveria então encontrar alguém que tivesse em suas propriedades uma produção de arroz e ao mesmo tempo ter interesse em adquirir animais, ou então deveria produzir seu próprio arroz. Como se pode perceber, nos deparamos com um primeiro problema, que podemos chamar de conflito de interesses. Qual a possibilidade de se encontrar alguém que tenha interesse em trocar certos commodities comigo, na quantidade que estou oferecendo? Tal limitação traria dificuldade no desenvolvimento econômico e tecnológico desta população.

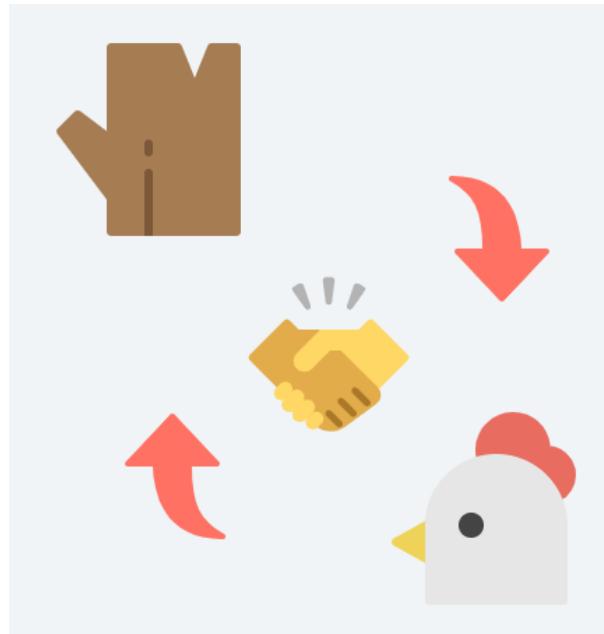
² Uma definição de dinheiro, segundo (KRUGMAN, 1984) “O dinheiro, argumentaram os economistas clássicos, serve a três funções: é um meio de troca, uma unidade de conta e uma reserva de valor”.

³ Uma definição bastante formal sobre dinheiro usada na escola austríaca de economia fica a cargo de (MISES, 1912):“Assim, haveria uma tendência inevitável para os menos comercializáveis da série de bens usados como meio de troca devem ser rejeitados um por um até que, finalmente, apenas uma única mercadoria permaneceu, que foi universalmente empregada como um meio de intercâmbio; em uma palavra, dinheiro”.

⁴ Se tormarmos uma abordagem mais filosófica, veremos que nem tudo são um mar de rosas. Segundo o apóstolo Paulo no primeiro livro de Timóteo afirma que o amor ao dinheiro é a raiz de toda a espécie de males; causador da cobiça de alguns que se desviaram da fé, e com muitas dores se trespassaram (BÍBLIA SAGRADA (ACF), 1994).

⁵ Segundo (GOLDBERG, 2005), o dinheiro fiduciário é uma moeda (um meio de troca ou transação) estabelecida como dinheiro, geralmente por regulamentação governamental. A moeda, de forma fiduciária, não tem valor intrínseco e não tem valor de uso. Tem valor apenas porque um governo mantém o seu valor ou porque as partes envolvidas na troca concordam com o seu valor.

Figura 1 – Escambo: Um acordo entre duas partes



Fonte: Desenvolvido pelo autor com assets disponíveis em (WHIMSICAL, 2021)

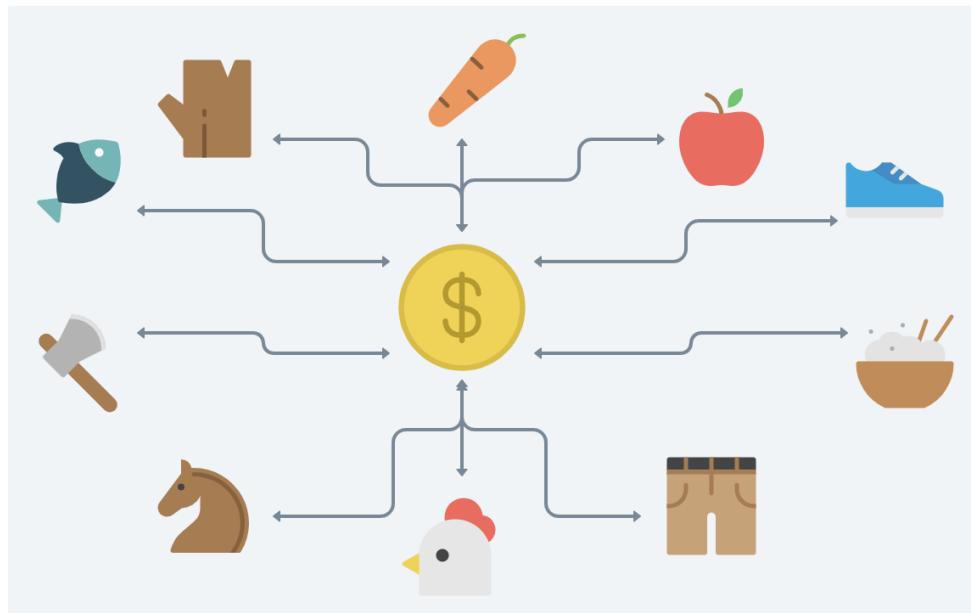
2.2.2 Conchas (e outros objetos)

Este foi um dos benefícios da ideia da objetificação monetária, que além de servir como um fomentador para a economia, permitiu a realização dos mais diversos tipos de transações, além de uma especialização da mão de obra. De fato, um lenhador poderia adquirir vestimentas, ferramentas e alimentos sem necessariamente ter que procurar alfaiates, ferreiros e fazendeiros que tenham interesse em madeira para isso pois a moeda passou a ser mais aceita pela população, permitindo escambos com um maior número de itens. Com isso, o lenhador não precisaria desenvolver suas próprias vestimentas e ferramentas e se especializar com técnicas de melhor extração de madeira e plantio de mais árvores, por exemplo.⁶

Embora possam parecer uma escolha bastante aleatória, as conchas tinham uma série de vantagens: eram semelhantes em tamanho, pequenas e duráveis. Enquanto os moluscos que produzem as conchas são encontrados nas águas costeiras dos oceanos Índico e Pacífico, a expansão do comércio fez com que até alguns países europeus aceitassem conchas como moeda. Conchas na forma de wampum (contas tubulares de conchas) foram usadas como dinheiro pelos nativos americanos. (TIKKANEN, 2020)

⁶ Na figura 2, a moeda de troca foi representada por uma moeda dourada, mas note que ainda não haviam moedas no tipo. Veremos mais sobre os metais na seção 2.3 abaixo

Figura 2 – Introdução ao dinheiro



Fonte: Desenvolvido pelo autor com assets disponíveis em (WHIMSICAL, 2021)

Perceba que não havia inicialmente um único tipo de moeda, uma lista longa de objetos serviu como moeda ao avançar dos tempos, sendo eles grãos de arroz, dentes de animais, animais e até escravos. Estes além de servir como forma de pagamento também tinham dois papéis importantíssimos: permitir a movimentação de recursos entre regiões mais afastadas geometricamente e também fixar os preços de todos os bens para uma única unidade. Ao passar do tempo, mais especificamente próximo do século VI A.C. as moedas metálicas foram tomando o lugar destes objetos devido a sua durabilidade, tamanho facilidade de divisão em partes menores e facilidade de transporte.

2.3 A jornada dos metais

Não poderíamos iniciar esta seção sem citar a numismática⁷, que é exatamente a área de estudo que trata do assunto aqui abordado. Continuando, artefatos metálicos, em sua majoritária parte obtiveram alta popularidade como meio de troca devido sua portabilidade, durabilidade e divisibilidade⁸, trazendo consigo as origens da cunhagem⁹.

⁷ Segundo o dicionário Dicio, numismática é a ciência que se dedica ao estudo de medalhas e moedas; numária ou numulária. Não só a ciência por trás deste estudo mas também pode ser relacionado como sinônimo ao colecionismo de tais moedas e medalhas. (7GRAUS, 2011)

⁸ Para facilitar a compreensão do leitor, tome nota do seguinte exemplo: uma moeda de hoje como 1 (um) BRL (um real brasileiro). Perceba que este pode ser dividido em 100 partes de centavo, cada uma valendo R\$ 0,01. Imagine a dificuldade e impraticabilidade de se dividir um animal vivo, como um boi, em incrementos pequenos o suficiente para realizar um escambo, ou como moeda de troca por um ramo de cenouras, por exemplo. Casos como estes são outra razão da popularidade dos metais em detrimento de peças vivas como animais, possibilitando assim espaço para a evolução da sociedade.

⁹ Segundo o dicionário Priberam, a cunhagem refere-se ao ato ou efeito de cunhar. Já cunhar refere-se ao ato de imprimir cunho num metal, originando moeda (ex.: cunhar euros; cunhar moeda), ou

Dependendo da região, a escolha do metal era determinada pela disponibilidade de acordo com esta região. No Egito antigo, apesar de não adotarem o uso de moedas de anéis de ouro no comércio exterior até o final do século 4 D.C., utilizavam barras de ouro desde o 4º milênio A.C., que mais tarde acabaram se desenvolvendo. Próximo ao Mar Egeu, lingotes de cobre conhecidos como talentos, eram originalmente uma unidade de peso de aproximadamente 55 a 70 libras (algo entre 25 kg e 31 kg) foram usados como moeda vários séculos antes da cunhagem. Na Grécia, a descoberta de uma barra de ferro com um punhado¹⁰ de espetos de ferro fracionários¹¹ serviu como moeda próximo de 1100 A.C. Ainda há outros exemplos de “moedas pesadas” também conhecidos como talentos¹². Ao prosseguir da história, nota-se o desejo de subdividir uma unidade pesada em frações menores para uso normal.

2.3.1 Cunhagem

Já segundo relatos históricos, a China foi o primeiro país a utilizar em suas transações objetos nos quais eu e você, caro leitor, reconheceria como um moeda. . Ainda assim, objetos como cochas confeccionadas por mãos humanas com materiais como o bronze, já existiam. Aqui estamos falando de 770 A.C. . Segundo citação de (YU; YU, 2004) no livro “Moedas chinesas: Dinheiro na história e na sociedade” (Tradução nossa):

À medida que o comércio se desenvolveu ainda mais e as fronteiras geográficas do comércio foram alargadas, a demanda por conchas naturais aumentou, e logo as conchas por si só não foram suficientes para atender à demanda. Em seguida, apareceram conchas de imitação criadas a partir de materiais feitos pelo homem. Um exemplo é a concha de bronze. Como as conchas de bronze eram facilmente unificadas em tamanho, peso e valor, elas foram imediatamente reconhecidas como superiores às conchas naturais. O aparecimento de conchas de bronze marcou o início da cunhagem de metal, que foi um grande passo à frente no desenvolvimento da economia jin. Devido ao rápido desenvolvimento econômico na primavera e outono e no Período dos Reinos Combatentes (770-221 a.C.), apareceram vários tipos de moedas. A forma de tais moedas imita formas de ferramentas agrícolas ou itens encontrados na vida diária. (Tradução nossa)

simplemente transformar em moeda (ex.: cunhar prata)(PRIBERAM, 2021)

¹⁰ Também conhecido como dracma

¹¹ Cujo nome é dado por obeloi

¹² Segundo (HUMPHREY; OLESON; SHERWOOD, 1997), o peso aproximado de um talento poderia variar de acordo com a região. Por exemplo, um talento grego, pesava 20,04kg (57 lb); um talento egípcio 27 kg (60 lb) e um talento romano pesava 32,3 kg (71 lb)

2.3.2 A primeira moeda oficial

Já a primeira região do mundo a usar procedimentos e instalações “industrializadas” para fabricar moedas que poderiam ser usadas como moeda de troca foi na região chamada Lídia, o que hoje seria considerada atualmente como Turquia ocidental, na europa. E ainda na Lídia, sob o reinado do rei Alyattes por volta de 610 A.C. surgiu o “Leão Lidiano”¹³, a primeira moeda oficial, justante cunhada com a efígie de um leão, símbolo da família real da Lídia, segundo os numismáticos. As moedas eram feitas de electro, uma liga ou mistura de origem natural de prata e ouro, e as vezes com vestígios de platina, cobre e outros metais.¹⁴

Figura 3 – O “Leão Lidiano”, a primeira moeda



NATIONAL
GEOGRAPHIC
PORTUGAL

Fonte: (NATIONAL GEOGRAPHIC, 2020)

¹³ Aqui estou fazendo uma tradução livre. Diversos textos em língua inglesa afirmam o nome “Lydian Lion” para a primeira moeda do mundo enquanto há poucas referências em português citando um nome para a moeda, referindo-a apenas como um estáter.

¹⁴ Você pode ler sobre este assunto em (MONTEREY, 2021)

Figura 4 – Mapa da Lídia de 1903



Fonte: (KIEPERT, 2013)

2.4 A transição para o papel moeda

Somente ao findar da dinastia Tang (618-907 D.C.) até a dinastia Song (960-1279 D.C.) ao iniciar do século VII na China pré-moderna é que o papel moeda surgiu como um meio de reduzir a necessidade de transportar os pesados e incômodos artefatos metálicas vistos até aqui para realizar transações. Se compararmos com os banco modernos, muito semelhantemente depósito eram feitos em entidades de confiança, e somente aí recebiam uma nota indicando quanto dinheiro haviam depositado. A nota poderia então ser resgatada em moedas de ouro e prata em uma data posterior. Segundo citação de (TIKKANEN, 2020): (tradução nossa):

Era feito da casca das amoreiras (então, em certo sentido, o dinheiro realmente crescia nas árvores). No final do século 18 e no início do século 19, o papel-moeda se espalhou para outras partes do mundo. O grosso dessa moeda, entretanto, não era dinheiro no sentido tradicional. Em vez disso, serviu como notas promissoras - promessas de pagar quantias específicas de ouro ou prata - que foram fundamentais para o desenvolvimento dos bancos.

Note que estes também poderiam ser trocados por bens e serviços e que eram emitidos por bancos e instituições privadas, não pelo governo, que agora é responsável pela emissão de moeda na maioria dos países, segundo (GRENVILLE; SELLWOOD, 2019). O papel moeda ainda perdurou por 500 anos até que a prática começasse a se popularizar na Europa no século 17. Ainda, o primeiro papel-moeda emitido por governos europeus foi, na verdade, emitido por governos coloniais na América do Norte. Relata-se que os colonos muitas vezes ficavam sem dinheiro à medida que as operações se expandiam pois os carregamentos entre

a Europa e as colônias da América do Norte demoravam demasiadamente.¹⁵ Com isso, em vez de voltar ao sistema de troca, os governos coloniais emitiam cartas assinadas¹⁶ com valores intrínsecos que passavam a ser negociados como uma moeda.

Figura 5 – Cartas assinadas

- (a) Carta de baralho assinada por entidade governamental para uso como moeda, 1729 (b) Regime francês, Reprodução de (a), 1714



Fonte: (BANK OF CANADA, 2019)

2.5 Guerras cambiais

Com a definitiva mudança para o papel moeda na Europa, os bancos e as classes dominantes começaram então a adquirir moedas de outras nações e criaram o primeiro mercado de câmbio, impulsionados pelo aumento das quantidades de transações internacionais possíveis. A capacidade dos países de negociar eram baseadas na estabilidade de seu governo ou monarquia, afetando assim o valor da moeda de sua nação. Isto acabou gerando competições entre os países, levando diversas vezes a guerras cambiais¹⁷, em que os países concorrentes encontravam métodos de alterar o valor da moeda do país

¹⁵ Voce pode ler mais sobre isto em (TEXAS REPUBLIC BANK, 2019)

¹⁶ Em inglês, um tipo deste documento é conhecido como IOU, documento que faz o reconhecimento da existência de uma certa dívida. Seu nome é uma fonética para “I owe you” (eu lhe devo, em português). Leia mais sobre isto em (KENTON, 2021)

¹⁷ Segundo o jornal BBC (PEIXOTO, 2010), o termo Guerra cambial é usado por diversos governos e economistas para descrever uma suposta disputa entre os países envolvendo suas moedas. O argumento é de que alguns países estariam impondo a desvalorização de suas moedas para beneficiar seus ganhos com exportação. Também pode referir-se como “Guerra monetária” e Guerra das moedas

concorrente elevando-a, encarecendo os bens do inimigo, reduzindo assim seu poder de compra¹⁸. Tome por exemplo a seguinte citação em (KEYNES, 1936):

Um dos primeiros exemplos da aplicação do argumento do desemprego como uma razão para a proibição das importações foi encontrado em Florença no ano de 1426. (...) Numerosos ataques foram dirigidos contra todas as pessoas que deveriam ter contribuído para uma exportação (excedente de exportação) de metais preciosos, ou para seu desaparecimento por causa de atividades correspondentes no país. (Tradução nossa)

O trecho é um exemplo do mercantilismo¹⁹, que ocorria quando as nações desejavam competir economicamente, envolvendo práticas para aumentar as exportações enquanto limitavam-se as importações. Com o desejo de aumentar a oferta de moeda doméstica e a riqueza das autoridades governantes, acontecendo especialmente por causa da necessidade de financiar guerras ou pagar dívidas, ocorria então a desvalorização da moeda.

Note que esta competitividade cambial ocorre até hoje, sendo um dos frutos de estudo de macroeconomia e preocupa investidores que têm interesse em fundos cambiais.

Figura 6 – Exemplos de moedas fiduciárias atuais



Fonte: (TIKKANEN, 2020)

2.6 Uma nova era: Cartões e ATMs

Com a evolução da tecnologia, dinheiro e pagamentos mudaram drasticamente a partir daqui. A tecnologia atual de processamento de cartões e as soluções de negócios avançadas tornam as transações financeiras possíveis de praticamente qualquer lugar de

¹⁸ Considere aqui também a capacidade de pagar para uma guerra, conforme visto no exemplo logo a seguir

¹⁹ Segundo (BEZERRA, 2020) O Mercantilismo foi o conjunto de ideias e práticas econômicas com objetivo de que a fonte de riqueza de uma nação se baseava no comércio com o mercado exterior e no acúmulo de metais preciosos.

forma instantânea. Tudo isto começou a ser possível a partir de 1871 quando a Western Union(WU)²⁰ deu lançamento as EFTs²¹, as transferências de fundos eletrônicos como método de pagamento para a troca de fundos. As EFTs tornaram-se populares como formas rápidas e fáceis de enviar dinheiro sem exigir uma troca física de dinheiro entre as partes remetentes e destinatárias tornando-se então a principal área de negócios da WU. Pouco menos de cem anos depois, já no final do século XX, surgiu um dos objetos mais importantes atualmente. Descrito como um pequeno cartão de plástico de precisamente 85,60 x 53,98 milímetros com cantos arredondados, que pode ser usado em praticamente qualquer lugar do mundo, ou online, para fazer pagamentos ou sacar dinheiro. Hoje chamamos este objeto de cartão de crédito ou débito. Mas não poderíamos deixar de citar que um pouco antes disto em 1967 na torre Enfield ao norte de Londres inaugurou-se então o primeiro caixa eletrônico (ATM)^{22,23}. Os ATMs são dispositivos de telecomunicações eletrônicas que permitem aos clientes de instituições financeiras realizar transações como saques em dinheiro, transferências, consultas de saldos e depósitos a qualquer momento do dia ou da noite e sem a necessidade de interação humana, ou seja, sem contato direto com funcionários de instituições financeiras.

Na época, os cartões bancários de plástico ainda não haviam sido inventados, então a máquina recebia cheques e distribuía apenas £10 por vez. (Sendo justo, isto vale cerca de £370 em dinheiro de hoje.) John Shepherd-Barron, que inventou o primeiro caixa eletrônico, morreu em 2010 um mês antes de seu 85º aniversário. Ele disse que a ideia foi inspirada em um dispensador de barra de chocolate. (Tradução Livre) (NELSON, 2018)

Hoje em dia os ATMs são muito conhecidos e utilizados por serem umas das formas principais de movimentação monetária física nos bancos. São conhecidos por estar presentes nos maiores estabelecimentos e estações de grande fluxo de pessoas como aeroportos, rodoviárias e centros comerciais.

2.7 Transações eletrônicas: dinheiro e bancos digitais

Ainda se tratando de tecnologia, devido a grande melhoria nas conectividades e nos hardwares dos dispositivos surgiu então uma nova forma de se tratar com dinheiro. Tal o conhecemos como o dinheiro digital, que refere-se a qualquer meio de pagamento gerenciado,

²⁰ Western Union é o nome pelo qual conhecemos a companhia hoje, seu nome em específico era então Western Union Telegraph Company

²¹ Do inglês, Electronic Fund Transfers, EFTs, que também eram conhecidos como wiring transfers.

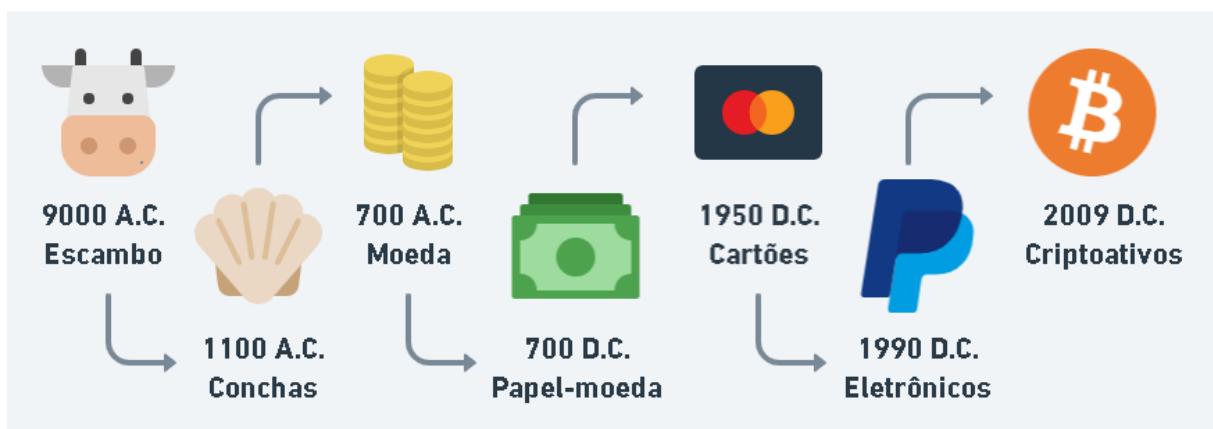
²² Também segundo (NELSON, 2018)

²³ A sigla ATM vem do inglês, que significa “Automated Teller Machine”. Os Tellers eram funcionários dos bancos que ficavam responsáveis por realizar as transações diretamente com os clientes bancários. No Brasil, a expressão “na boca do caixa” representa bem essa interação com os tellers.

armazenado ou transacionado de forma eletrônica por meio de sistemas computadorizados, especialmente pela Internet. Um marco na evolução dos pagamentos digitais ocorreu em 1998 com o lançamento do Paypal²⁴, que permitia a transferência e armazenamento de valores eletrônicos em carteira eletrônica, iniciando uma febre nesse ramo. No Brasil, a digitalização das operações financeiras deu início com o surgimento dos boletos bancário no fim dos anos 90 e da Transferência Eletrônica Disponível²⁵ (TED), logo no início dos anos 2000, mas seu grande fomento surgiu no começo dos anos 2010, quando surgiram os primeiros bancos digitais no Brasil, que chegaram com fortes diferenciais para a época, como a gratuidade em diversos serviços como transferências entre contas, documentos de crédito(DOCs) e TEDs, alguns tipos de investimento, rendimento acima da Poupança na própria conta corrente, além de outros diferenciais como cartão de crédito sem anuidade e conta corrente totalmente gratuita.²⁶ As fintechs, como são conhecidas tais instituições financeiras, puderam gerar uma maior evolução das instituições tradicionais devido a concorrência fazendo ainda que tais empresas criassem suas próprias versões digitais.

No próximo capítulo falaremos sobre um subconjunto do dinheiro digital, o dinheiro virtual.

Figura 7 – Resumo do capítulo em uma imagem



Fonte: Desenvolvido pelo autor com assets disponíveis em (WHIMSICAL, 2021)

²⁴ De acordo com (CANALTECH, 2020), Fundada por Max Levchin, Peter Thiel, Luke Nosek e Ken Howery, a PayPal foi criada, inicialmente, como uma solução para pagamentos via Palm Pilot. Após a fusão com a X.com, o PayPal passou a atuar na internet, tornando-se uma das plataformas de pagamentos online mais populares do mundo. Atualmente oferece um sistema de pagamentos on-line que é uma alternativa eletrônica aos métodos de pagamento tradicionais, como cheques e ordens de pagamento.

²⁵ O TED foi introduzido em 23 de abril de 2002 pela circular nº 3.115 do Banco Central do Brasil. Veja em (BANCO CENTRAL DO BRASIL, 2002)

²⁶ Leia mais sobre a digitalização dos bancos em (DOMINA CONCURSOS, 2021)

Capítulo 3

O futuro: cripto

“O que me afetou mais profundamente foi a percepção de que as ciências da criptografia e da matemática são ciências puras muito elegantes. Descobri que os fins para os quais¹ essas ciências puras são usadas são menos elegantes.” - Jim Sanborn (tradução livre)

Neste capítulo mostraremos sobre o dinheiro do futuro, os criptoativos, relatando sua concepção e uma visão geral sobre este tema. Mas antes faremos uma revisão rápida sobre criptografia.

3.1 Uma noção rápida sobre criptografia

3.1.1 Idéia geral

A criptografia pode ter várias definições^{2,3}. Como podemos notar observando estas definições, o início da história da criptografia data-se a medida que seres humanos iniciaram organizar em tribos, no qual já havia a necessidade de se comunicar, uma consequência disto seria a necessidade da comunicação em segredo. Na criptografia moderna, não

¹ Citação original do inglês: “What affected me most profoundly was the realization that the sciences of cryptography and mathematics are very elegant pure sciences. I found that the ends for which these pure sciences are used are less elegant.” em entrevista com Milena Kalinovska (SANBORN, 2003)

² Segundo o dicionário Oxford (OXFORD UNIVERSITY PRESS, 2021), criptografia nada mais é que a arte de escrever ou resolver códigos.

³ Conforme definido por (RIVEST, 1990), criptografia é a prática e o estudo de técnicas para comunicação segura na presença de comportamento adverso

há somente a preocupação na resolução de problemas provenientes de ataques internos ou externos, mas também na melhoria da segurança digital sobre dados, informações, transações e computações distribuídas⁴. Mais especificamente também são estudados autenticação de mensagens, assinaturas digitais, protocolos para troca de chaves secretas, protocolos de autenticação, dinheiro digital, leilões eletrônicos e eleições. Até o final do século XX, a criptografia era considerada uma forma de arte, somente depois desse período ela começou a ser estudada de forma mais formal, com o desenvolvimento de uma teoria, sendo considerada assim uma ciência.

A criptografia possui quatro objetivos:

Objetivos da criptografia	
Confidencialidade	Somente o destinatário autorizado deve ser capaz de extrair o conteúdo da mensagem da sua forma cifrada.
Integridade	O destinatário deverá ser capaz de verificar se a mensagem foi alterada durante a transmissão.
Autenticação	O destinatário deverá ser capaz de verificar que se o remetente é realmente quem diz ser.
Irretratabilidade	Não deverá ser possível ao remetente negar a autoria de sua mensagem.

Tabela 1 – Objetivos gerais da criptografia

3.1.2 Métodos criptográficos históricos

Se considerarmos uma criptografia pré-computacional, existem basicamente dois métodos para esconder as informações de uma mensagem. São eles a transposição e a substituição dos caracteres. Tais execuções poderiam então ser operadas pelo emissor e pelo destinatário da mensagem.

- No método da transposição, os conteúdos da mensagem criptografada e da mensagem original são idênticas, o que muda são a disposição das letras da mensagem.

⁴ Pode-se entender computação distribuída como um sistema de processamento distribuído, ou seja, um sistema possuindo de múltiplos nós de processamento, porém interligados como um único sistema computacional. Veja (PROGRAMAÇÃO PROGRESSIVA, 2021) para saber mais

- No método por substituição cada letra permanece em seu devido lugar, porém ocorre uma substituição de acordo com uma tabela de referência que podem conter também figuras e símbolos.

A cifra de César, que no caso trabalha com um valor fixo de saltos nas posições das letras do alfabeto é um exemplo clássico de criptografia por chave de substituição. O formato de medalhão pode ser facilmente adquirido atualmente conforme figura abaixo:

Figura 8 – Medalhão de cifra de César disponível para venda



Fonte: (RETRWORKS, 2021)

3.1.3 Chaves criptográficas

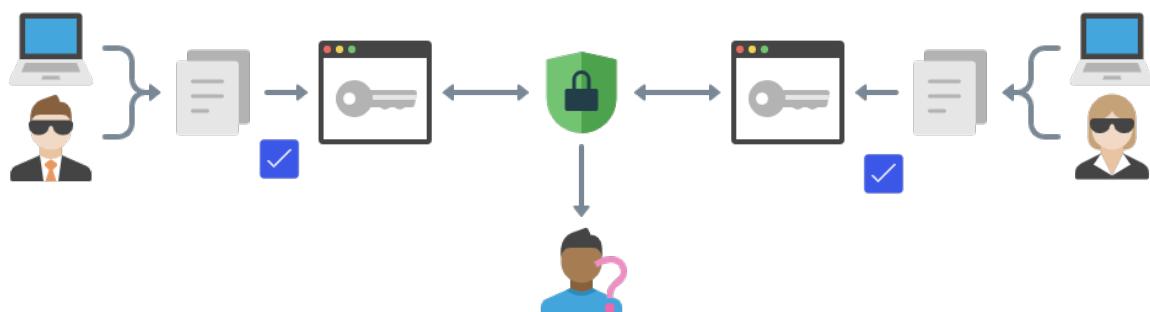
Como pode-se notar, um algoritmo matemático fica responsável pelo segredo⁵ da chave criptográfica e é o segredo fundamental da criptografia. Existem dois tipos de chaves, conforme tabela:

⁵ Tal algoritmo criptografa a mensagem do remente e descriptografa ao chegar no destinatário

Tipos de chaves criptográficas	
Privada (Simétrica)	Somente o proprietário de uma chave única é capaz de decifrar a mensagem
Pública e privada (Assimétrica)	Neste caso se utilizam duas chaves, uma delas é utilizada para criptografar e a outra para descriptografar as mensagens. Como a chaves tem relações, se a ação de uma chave é engatilhada, somente o seu par poderá desfazer tal ação. Com isso, a chave pública pode ser trazida a público e somente a chave privada fica sobre restrição do destinatário.

Tabela 2 – Tipos de chaves criptográficas

Figura 9 – Esquema de funcionamento das criptografias por chave pública e por chave privada



Fonte: Desenvolvido pelo autor com assets disponíveis em (WHIMSICAL, 2021)

3.1.4 A tecnologia blockchain

O blockchain surgiu como uma forma de organizar de forma segura as transações com criptomoedas de forma imutável. Imagine o Blockchain como um grande banco de dados distribuído, um livro-caixa de registros de transações, onde aquilo que é registrado não pode ser alterado sendo então uma forma segura de compartilhamento entre redes e usuários, sendo gerenciados de forma autônoma⁶. Se tratando de educação financeira, a tecnologia de blockchain tem grande potencial de aumentar a literacia e o interesse geral da população sobre os criptoativos.

⁶ De tal forma que não há um mestre administrador, todos aqueles que utilizam do sistema são administradores.

3.2 Os criptoativos

3.2.1 Conceito

Os criptoativos são moedas virtuais. Moedas virtuais são um valor monetário representado unicamente por forma eletrônica. Assim como o dinheiro digital, estes também são gerenciados, armazenados ou transacionados de forma eletrônica por meio de sistemas computadorizados, especialmente pela Internet, porém estes não possuem uma contrapartida física. Por exemplo, a quantidade de reais em sua conta bancária online hoje são dinheiro digital porque eles assumem uma forma física quando você os saca em um ATM, diferente do dinheiro virtual. Estes são emitidos por grupos de desenvolvedores ou empresas privadas e, em sua grandíssima maioria, não são regulamentadas. Chamamos estas de descentralizadas.

3.2.2 Concepção

A razão pelo qual este capítulo iniciou falando sobre criptografia é porque as criptomoedas utilizam da criptografia para sua segurança. O Bitcoin foi a primeira implementação do conceito hoje conhecido como criptomoeda, cujo foi descrito inicialmente em 1998 por Wei Dai na lista de mala direta de discussão cypherpunks⁷, sugerindo a ideia de uma nova forma de dinheiro que usa criptografia para controlar sua criação e transações, ao invés de um autoridade central. A primeira especificação e prova de trabalho(PoW)^{8,9} do Bitcoin foi publicada em 2009 em uma lista de discussão de criptografia por Satoshi Nakamoto. Satoshi deixou o projeto no final de 2010 sem revelar muito sobre si mesmo. A comunidade cresceu exponencialmente com muitos desenvolvedores trabalhando em Bitcoin. (THE BITCOIN PROJECT, 2021)

⁷ Um cypherpunk é qualquer indivíduo que defende o uso generalizado de criptografia e tecnologias que aumentam a privacidade no objetivo de se obterem mudanças sociais e políticas. Sua comunicação original deu-se por meio da lista de mala direta Cypherpunks, que uniam grupos informais que almejavam privacidade e segurança por meio do uso intenso de criptografia.

⁸ Aqui estou fazendo uma tradução livre. Segundo (FRANKENFIELD, 2021) uma “proof of work” ou uma prova de trabalho é uma evidência de que um certo poder computacional foi utilizado para resolver um desafio matemático arbitrário em um sistema controlado. As provas de trabalho são amplamente utilizadas hoje em dia na mineração de criptomoedas, para validar transações e minerar novos tokens.

⁹ Segundo (NAKAMOTO, 2008) , O protocolo PoW envolve escanear um valor utilizando a função hash, como a função SHA-256, onde o hash começa com n bits de valor 0 (Veremos rapidamente sobre esta notação no capítulo de aplicação de atividade). O trabalho médio requerido é exponencial ao número de bits 0 e podem ser verificados utilizando um único hash.

3.2.3 Receptividade no mundo e na sociedade brasileira

3.2.3.1 No mundo

Como já foi citado anteriormente, por enquanto a descentralização continua sendo uma atribuição frequente aos criptoativos devido ao seu curto tempo de existência, sendo uma vantagem segundo os investidores devido a privacidade e a fuga de burocracias e taxas possibilitadas pela independência de intermediários. Segundo (NPARTNERS, 2021), os bancos centrais de diferentes países têm intensificado críticas, argumentando que o dinheiro digital têm poucos mecanismos para resgate e que “operam contra o bem público”.

Apesar disso, as criptomoedas não são ilegais pois atuam em um vácuo de legislação sobre o tema a nível mundial. A tecnologia opera como acordo mútuo entre duas partes, que concordam que a moeda tem valor e que podem estar em qualquer lugar do mundo. (NPARTNERS, 2021)

3.2.3.2 No Brasil

Até o presente momento as criptomoedas ainda não são regulamentadas, mas já há uma maior aceitação por parte das autoridades¹⁰ e do banco central brasileiro e o governo quando se tratam deste tema se compararmos com algumas dissertações sobre este tema de anos anteriores.

Segundo o presidente Gilson Finkelsztain da bolsa de valores brasileira, a *B3*, “É natural que façamos expansão para o mundo não regulado das criptos” e que segundo ele, já há alguns planos que a *B3* pretende oferecer infraestrutura para negociação de criptoativos. “Não é uma bolsa de cripto, mas entrar nesse mercado para oferecer serviços para quem negocia cripto”, explicou. (TOLOTTI, 2021)

E seguindo para uma tendência na tecnologia de blockchain, segundo (BARCELLOS, 2021) o banco central brasileiro já tem planos de ampliar as formas de pagamento no país criando sua própria CDBC¹¹, entitulada real digital, uma moeda virtual cujas expectativas são o aumento da inovação, criando soluções que não eram viáveis com o dinheiro em papel ou então barateando soluções que já estão em regime de produção. Ainda segundo a reportagem,

¹⁰ Recentemente, um projeto de lei (**PL**) uma proposta pela tentativa de regulamentação das criptomoedas foi aprovada na câmara dos deputados. Segundo a reportagem veiculada em (BRASIL, 2021), o objetivo da lei é a prevenção da lavagem de dinheiro e o combate às fraudes. Até o fim da edição deste documento, o PL ainda segue para averiguação do senado federal.

¹¹ CDBC é uma sigla que vem do inglês que significa Central Bank Digital Currency, ou moeda digital de banco central, que como o próprio nome cita, são moedas centralizadas controladas por uma única entidade, um banco central.

3.2.4 Proposta de modelo de pesquisa (com questionário)

Ao desenrolar do desenvolvimento deste instrumento, o autor depara-se com a notícia veiculada em (AGÊNCIA DINO, 2021), que afirma que 99% dos brasileiros não conseguem passar em uma avaliação de conhecimento básico de criptomoedas. A avaliação permitia que pessoas de todo o mundo pudessem testar seu nível de compreensão sobre criptomoeda e identificar onde elas precisam aprimorar o conhecimento.

Como mostra a taxa de aprovação do questionário, existe uma lacuna significativa do conhecimento no Brasil, México e EUA. Nos EUA, quatro em cada 10 entrevistados não conseguiram responder a mais da metade das perguntas, escolhendo 'não sei'. No entanto, os americanos tiveram um desempenho melhor do que os brasileiros, com três em cada 10 respondendo corretamente a cerca de um terço das perguntas do questionário. No geral, os países têm taxas de adoção semelhantes (14% no México, 15% no Brasil, 17% nos EUA). (AGÊNCIA DINO, 2021)

Um dos objetivos gerais ¹² deste instrumento é disseminar criptoliteracia que é o conhecimento sobre criptomoedas argumentando sobre suas funções e características para que na esperança de em algum momento no futuro estes sejam acessíveis e de fácil compreensão, independentemente da renda, status educacional ou sexo, com isso propõe-se uma pequena pesquisa para averiguar em uma escala, de forma local e ainda menor do que adotada pela reportagem, sobre o tema¹³.

3.2.4.1 Resolução do teste rápido apresentado

As cinco questões aqui apresentadas foram adaptadas da pesquisa oficial disponível na reportagem para que haja uma melhor contextualização dos leitores. Não obstante, se o participante responde qualquer opção diferente de “Nunca ouvi falar” na questão sobre sua familiaridade com os criptoativos, este então segue o fluxo usual para a seção do teste. Seguem então suas respostas:

Pergunta: Quais destas frases melhor descreve um criptoativo?

- Dinheiro que pode ser armazenado fisicamente ou eletronicamente

Sim, apesar de existirem carteiras físicas para armazenamento de criptoativos, esta não é a melhor alternativa.

- Dinheiro em papel que só podem ser usados para transações físicas

Esta alternativa é incorreta pois os criptoativos não são feitos de papel-moeda.

¹² Visto na seção 1.3

¹³ Antes de prosseguir para a subseção (3.2.4.1), recomenda-se ir até a seção do apêndice(5.2), onde a pesquisa está disponível para consulta

- **Uma moeda digital ou virtual protegida por criptografia**

Correto! Esta alternativa é a melhor opção pois cita a criptografia, base fundamental dos criptoativos.

- **Moeda que só pode ser usada para remessas internacionais**

Esta alternativa é incorreta pois apesar das criptomoedas serem uma excelente opção para remessas internacionais, estes não ficam limitadas somente nesta função.

- **Eu não sei**

Opção que indica que o participante prefere não arriscar uma resposta.

Pergunta: Quais destes você acredita que não seja uma criptomoeda?

- **Ethereum**

Opção incorreta. O Ethereum (ETH) é uma criptomoeda descentralizada que teve seu lançamento em 2015.

- **Litecoin**

Opção incorreta. O Litecoin (LTC) é uma criptomoeda muito semelhante ao bitcoin que teve seu início em 2011.

- **Dogecoin**

Opção incorreta. O Dogecoin (DOGE) é uma criptomoeda que foi criada com a temática do meme Doge, um cachorro da raça shiba inu.

- **Metamask**

Opção correta! O metamask é uma carteira digital que permite guardar e transacionar criptomoedas e não uma criptomoeda em si.

- **Stellar Lumens**

Opção incorreta. O Stellar Lumens (XLM) é uma criptomoeda criada em 2014.

- **Eu Não sei**

Opção que indica que o participante prefere não arriscar uma resposta.

Pergunta: O que é a mineração de criptomoedas?

- Uma rede de carteiras físicas e digitais enviando e recebendo ativos digitais entre si, mantendo a segurança do blockchain, é o processo que aumenta a quantidade de moedas em circulação.

Opção correta! Esta opção é a que melhor define a mineração de criptoativos.

- Um aplicativo de telefone onde os usuários resolvem ou jogam jogos e recebem criptomoedas como recompensa

Opção incorreta.

- O processo de mineração de metais preciosos para financiar o desenvolvimento de um projeto de criptografia

Opção incorreta. O termo “minerar” também pode ser usado na extração de minério, mas não tem relação direta com a mineração de criptoativos.

- Eu não sei

Opção que indica que o participante prefere não arriscar uma resposta.

Pergunta: Moedas regulamentadas, apoiadas por bancos centrais, tem divisibilidade limitada. Um real, por exemplo, só pode ser dividido em 100 partes de centavo, cada uma valendo R\$ 0,01. Quantas unidades, ou casas decimais, um bitcoin pode ser dividido?

- 3 casas decimais

Opção incorreta.

- 8 casas decimais

Opção correta! Um bitcoin é divisível em oito casas decimais (100 milionésimos de um bitcoin), e esta menor unidade é denominada de um Satoshi em homenagem ao seu criador, Satoshi Nakamoto.

- 20 casas decimais

Opção incorreta.

- Nenhum. Você não pode dividir um bitcoin em um decimal

Opção incorreta.

- Eu Não sei

Opção que indica que o participante prefere não arriscar uma resposta.

Qual métrica é usada para medir o poder de processamento de uma rede de mineração de criptomoedas?

- CPUs

Opção incorreta. CPUs são denominados por Central Process Unit, ou Unidade Central de Processamento. São o principal componente de hardware de um computador.

- Hashrates (h/s)

Opção correta! Hashes por segundo indicam a quantidade de operações computacionais que um sistema ou rede de mineração é capaz de realizar em um segundo.

- Megahertz (MHz)

Opção incorreta.

- Gigahertz (GHz)

Opção incorreta.

- Eu Não sei

Opção que indica que o participante prefere não arriscar uma resposta.

Capítulo 4

Proposta de atividade e *Hands on!*

“Montamos uma pequena operação de mineração de bitcoin e ethereum... que milagrosamente agora está ganhando muito¹. dinheiro” - Abigail Johnson (tradução livre)

Neste capítulo é exibida uma atividade desenvolvida pelo autor do presente instrumento que mostra aos alunos o custos e ganhos na mineração de criptomoedas, além do cálculo do tempo de retorno do investimento de um hardware apropriado.

4.1 Introdução

Neste capítulo, uma simples proposta de atividade será apresentada. Esta atividade pode ser aplicada com discentes do ensino fundamental e envolve conhecimentos de matemática financeira, conversões de medidas, sobre capacidade computacional de computadores e ainda há a oportunidade da interdisciplinaridade com turmas de história², turmas de geografia³, ou até em turmas de língua inglesa ou língua espanhola⁴.

A ideia da atividade é introduzir ao aluno sobre a existência de algoritmos de mineração já bastante difundido pela comunidade de mineração, como por exemplo *Ethash*, *Ethash4G*, *KawPow* e *MTP* e juntamente com a calculadora de lucros *Whattomine*⁵ obter alguns

¹ Citação original do inglês: “We set up a small bitcoin and ethereum mining operation... that miraculously now is actually making a lot of money.” em reportagem (SHIEBER, 2017)

² Aqui supondo alguma base histórica sobre valores monetários, história da criptografia

³ Conceitos de globalização ou circulação de capital se aplicam bem aqui

⁴ Aqui podemos explorar que a mineração pode ocorrer em qualquer lugar do mundo, estudar sobre como a leitura de website em língua inglesa ou espanhola podem abrir novas possibilidades para os alunos

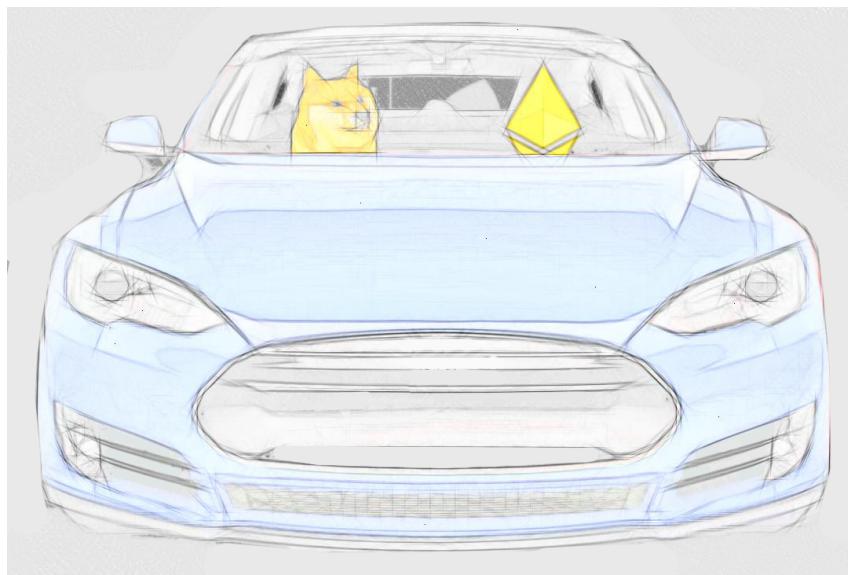
⁵ Você pode aprender mais sobre esta ferramenta acesso seu endereço em (WHATTOMINE, 2020)

cálculos convertendo gasto energético em lucro. Por último, gostaríamos de estimar o tempo estimado da recuperação dos investimentos em hardware, novamente segundo os cálculos da calculadora de lucros e uma tabela de cálculo desenvolvida pelo autor deste presente instrumento.

4.1.1 Motivador para a atividade

Você leitor, tem interesse em minerar criptomoedas e não sabe calcular se essa atividade “vale a pena”? Com as altas taxas de desemprego atualmente em nosso país, muitas pessoas hoje em dia já estão fazendo rendas extras e até como renda principal a mineração de criptomoedas. Imagine a seguinte situação: Um motorista por aplicativo para adquirir um veículo novo deve investir uma média de 20 a 30 mil reais. Supondo que este motorista tenha uma certa renda bruta, excluiria-se daí então uma grande porção em combustível, taxas veiculares, multas e manutenções, excluindo ainda o fator segurança. Em quanto tempo este motorista recuperaria seu investimento? Ao final deste capítulo, um comparativo será possível.

Figura 10 – Um passeio veicular com Dogecoin e Ethereum



Fonte: Ilustrado digitalmente pelo autor

4.2 Embasamento da atividade

4.2.1 Bases necessárias para a atividade

Conforme relatado no plano de aula do professor, recomenda-se que o conteúdo desta atividade seja inserido num cronograma de aulas de matemática financeira. Conversões de

câmbio, conversões de medidas e porcentagens são alguns dos termos que serão usados.

4.2.1.1 Matemática Financeira

A atividade é baseada na importância dos alunos terem um boa literacia, ou letramento financeiro. Segundo (ORTON, 2017), literacia:

Refere-se à capacidade de ler, analisar e interpretar as condições financeiras pessoais que afetam o bem-estar em nível material. Inclui a capacidade de discernir sobre decisões financeiras, discutir sobre dinheiro e assuntos financeiros. Planejar o futuro e responder de forma competente às várias etapas e acontecimentos da vida que afetam as decisões financeiras, incluindo acontecimentos da economia em geral.

Tal literacia traz um interesse geral tanto para empresas multinacionais tanto para governantes, pois uma nação cuja população possui um ensino rígido em Educação financeira (**EF**) tem fundamentos para que haja a promoção do crescimento econômico, confiança e estabilidade e complexidade dos mercados financeiros. Segundo o (OCDE, 2005), a educação financeira pode ser definida como o processo pelo qual os consumidores/investidores financeiros melhoram sua compreensão de produtos, conceitos e riscos financeiros e através de informações, instruções e/ou conselhos objetivos, desenvolver as habilidades e a confiança para se tornar mais consciente dos riscos e oportunidades financeiras, para fazer escolhas informadas, para saber onde buscar ajuda e tomar outras medidas eficazes para melhorar seu bem-estar financeiro.

Com efeito, tudo começa com o hábito, e para isso, precisamos ter uma compreensão profunda dos hábitos que podem impactar a capacidade financeira no decorrer da vida e ensinar os alunos ainda pequenos sobre educação financeira faz parte deste processo de crescimento econômico nacional.

4.2.1.2 Conversões de medidas

A necessidade de se tomar medidas são muito antiga e se remetem ainda as civilizações primárias. De fato, cada população tinha seu jeito de tomar medidas, onde muita das vezes tais unidades eram imprecisas pois tinham base no corpo humano como pé, polegada, jarda, braça, côvado, palmo, etc. Alguns destes tipos de medição podem ser facilmente encontrados em livros históricos como visto em (CUNHA, 2011) e são conhecidos atualmente no sistema imperial⁶, diferente do sistema internacional de medidas (SI) padronizado que conhecemos⁷.

⁶ Alguns destes como pés, polegadas e jardas são amplamente usado em países como os Estados Unidos da América.

⁷ Leia mais sobre isto em (LEGER, 2019)

Nesta atividade usaremos a escala de armazenamento computacional e também a escala de hashes, conforme abaixo.

Abreviação	1 h/s	1 KH/s	1 MH/s	1 GH/s	1 TH/s	1 PH/s	1 EH/s
Leitura	1 hash por segundo	1 kilohash por segundo	1 meghash por segundo	1 gigahash por segundo	1 terahash por segundo	1 petahash por segundo	1 exahash por segundo
Referência	Unidade base	Mil hashes por segundo	Um milhão de hashes por segundo	Um bilhão de hashes por segundo	Um trilhão de hashes por segundo	Um quadrilhão de hashes por segundo	Um quinquilhão de hashes por segundo

Tabela 3 – Tabela de conversão de hashes

Abreviação	1 B	1 KB	1 MB	1 GB	1 TB	1 PB	1 EB
Leitura	byte	kilobyte	megabyte	gigabyte	terabyte	petabyte	exabyte
Referência	Unidade base equivalente a 8 bits	1024 B	1024 KB	1024 MB	1024 GB	1024 TB	1024 PB

Tabela 4 – Tabela de conversão de armazenamento computacional

4.2.2 Embasamento de construção

4.2.2.1 Acadêmico

Em relação ao embasamento acadêmico para esta atividade vamos tomar como referência algumas habilidades previstas na Base Nacional Comum Curricular (**BNCC**). Segundo a BNCC :

(EF09MA18) Reconhecer e empregar unidades usadas para expressar medidas muito grandes ou muito pequenas, tais como distância entre planetas e sistemas solares, tamanho de vírus ou de células, capacidade de armazenamento de computadores, entre outros.

(EF08MA04). Resolver e elaborar problemas, envolvendo cálculo de porcentagens, incluindo o uso de tecnologias digitais

(EF05MA19) Resolver e elaborar problemas envolvendo medidas das grandezas comprimento, área, massa, tempo, temperatura e capacidade, recorrendo a transformações entre as unidades mais usuais em contextos socioculturais.

A atividade toma base do que está por trás do conceito chave da habilidade EF09MA18 onde os alunos consigam aplicar os conceitos de escalas computacionais partindo da ideia que todo computador codifica sua informações em base binário⁸, no qual 1 byte equivale 8 bits. O bit é a unidade base de armazenamento nas memórias dos computadores. Para que haja sucesso nesta aplicação os discentes deverão ter domínio das habilidades EF08MA04, que trata da capacidade de calcular porcentagens onde em nosso problema queiramos encontrar as proporcionalidades entre o valor total investido e valor do lucro mensal, tomando com variável temporal os meses de trabalho do hardware e da habilidade EF05MA19, mais especificamente da grandeza de capacidade.

4.2.3 Infraestruturas digitais

4.2.3.1 On premise versus cloud

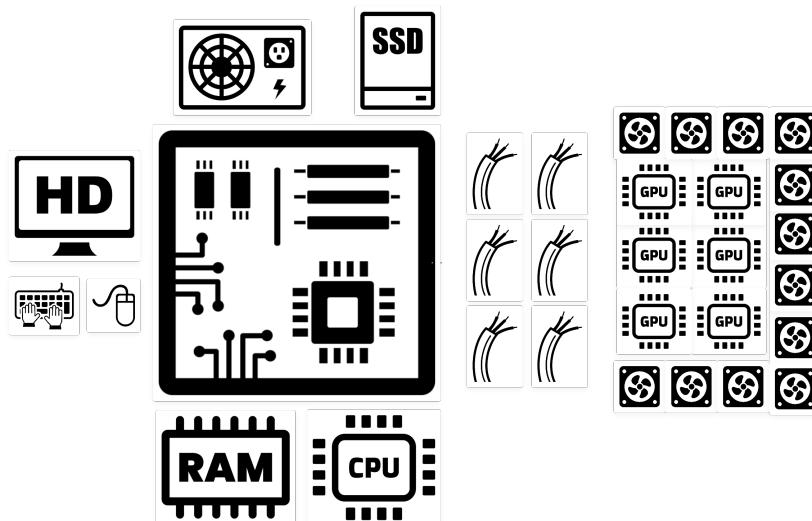
Na engenharia de dados é muito comum a discussão entre estes dois modelos de gestão de hardware e ao passar dos anos muitas empresas tem investido em campanhas e jornadas com o objetivo de migrar seus sistemas on-premises⁹ para sistemas em nuvem¹⁰. Todas as suposições orçamentárias discutidas nesta atividade tomam como referência uma arquitetura física, ou seja on-premise.

⁸ A Base binária é representada por zeros (0) e uns (1)

⁹ Uma infraestrutura On premise é aquela em que o próprio usuário ou empresa possui toda e qualquer responsabilidade de processar suas aplicações de software e hardware. Ou seja, toda refrigeração, configuração, customização e atualização é feita de modo interno, dentro de suas dependências. Mais ainda, o usuário é responsável por reservar um espaço físico adequado e cuidados contra incêndios, inundações, desabamentos e roubos.

¹⁰ Uma infraestrutura é considerada em cloud (Do inglês, nuvem) se tanto hardware e software estão remotos, ou seja, fora das dependências do usuário ou empresa. Em geral, tais serviços são oferecidos por empresas especializadas para esse fim. Nesta modalidade, paga-se pelo consumo dos poderes computacionais, como disco e memória.

Figura 11 – Arquitetura de um RIG



Fonte: Desenvolvido pelo autor com assets open-source

4.2.3.2 Sistemas operacionais

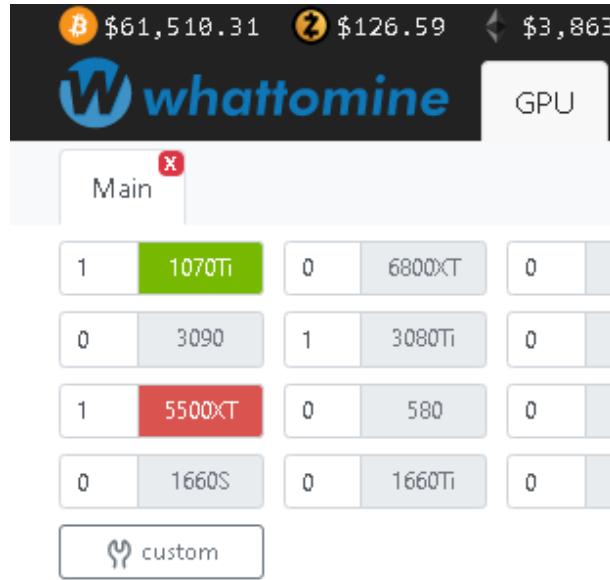
O sistema operacional no qual o aluno faz a pesquisa é indiferente uma vez que as ferramentas de pesquisa a serem utilizadas funcionam de forma igual em todos os sistemas operacionais. Já o sistema operacional que é instalado no equipamento não tem seus custos considerados pois existem excelentes opções open-source que não possuem perdas de desempenho se comparados com seus concorrentes.

4.3 Guia para o professor e guia para o *Hands on!*

Caro professor, a seguir você terá algumas orientações para uma melhor desenvolvimento desta atividade. Sem perda de generalidade, vamos estipular como objetivo iniciar no seu interesse em minerar a criptomoeda ETH, que possui grande abrangência de conhecimento na comunidade e possui atualmente a maior lucratividade média de acordo com sua dificuldade de obtenção. Nesta atividade usaremos a calculadora de lucros *Whattomine*¹¹, que possuem as práticas mais simplificadas para esta atividade. Primeiro, inicie navegando para (WHATTOMINE, 2020). Em seguida, pode-se sugerir que um aluno selecione um modelo de placa de vídeo. Quando uma GPU *Nvidia* for selecionado, o botão se tornará verde, e quando uma GPU *AMD* for selecionado, o botão se tornará vermelho. Isto auxilia o alunos no momento da pesquisa de preços pois um bom padrão de pesquisa pode ser “<marca> + <modelo> + <preço> ”

¹¹ O professor pode utilizar outras calculadoras disponíveis conforme 13

Figura 12 – Guia de cores dos botões de seleção de GPUs



Fonte: (WHATTOMINE, 2020)

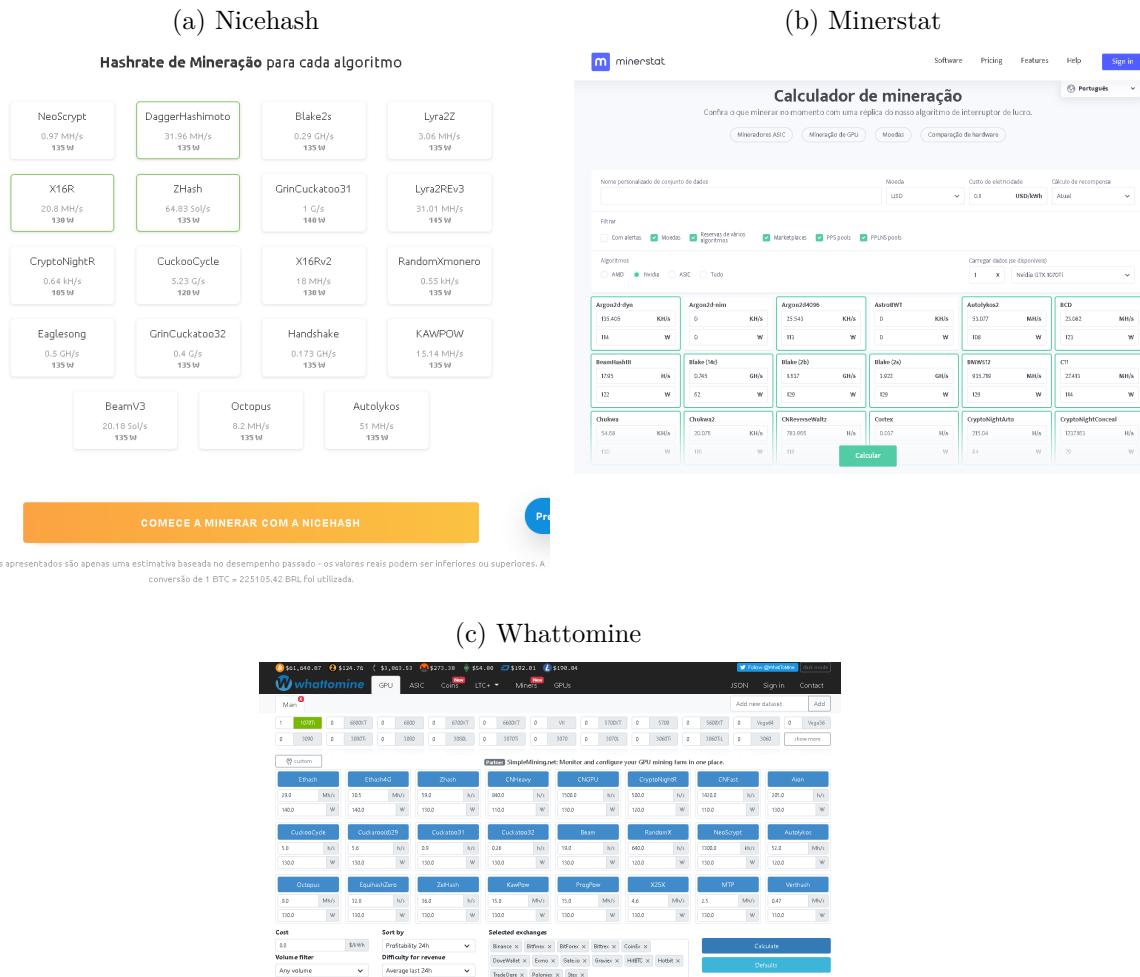
Para padronização dos procedimentos e simplificação dos cálculos, definimos então somente uma unidade do modelo selecionado e não consideremos inicialmente os custos energéticos. Tais cálculos serão feitos na planilha piloto. Como nosso objetivo é minerar ETH¹², selecionemos os dados no campo ethash

Figura 13 – Outras opções da calculadoras

Fonte: (NICEHASH, 2021) e (MINERSTAT OÜ, 2021)

¹² Uma forma de variação desta atividade é que cada aluno faça um comparativo das diferentes criptomoedas com um mesmo equipamento

Figura 14 – Exemplos de diferentes algoritmos de mineração disponíveis nas calculadoras



Fonte: (NICEHASH, 2021), (MINERSTAT OÜ, 2021) e (WHATTOMINE, 2020)

Conforme a tabela disponível na calculadora logo abaixo das opções, tomemos então nota.

4.3.1 Orientações gerais para uso da planilha piloto

- Para calcular de forma simples o valor do kilowatt/hora no mês específico basta tomar nota o valor total da conta e dividir pelo número de kilowatts gastos no referente mês. Tome nota que existem fatores que podem aumentar ou diminuir este valor para outros meses, sendo este o sistema bandeiras tarifárias, que indicam se haverá ou não acréscimo no valor da energia a ser repassada ao consumidor final, em função das favorabilidade da geração de eletricidade, aumento ou abatimento de impostos municipais, estaduais e federais, entre outros.
 - O consumo energético mensal é calculado da seguinte forma: Toma-se o consumo em kW de uma GPU, multiplica-se pelo número de GPUs na RIG, e deste valor soma-se

o fator de consumo do RIG que nada mais é que o consumo esperado dos outros componentes do RIG fora as GPUs. Este valor tem base empírica.

- A cotação de USD para BRL acontece de forma automática pelo serviço gerenciado da google. Por isso, há um aviso de exoneração abaixo afirmando que “As cotações não são provenientes de todos os mercados e podem ter um atraso de até 20 minutos. As informações são fornecidas “no estado em que se encontram” e apenas para fins informativos, não para fins comerciais ou consultoria”.

$$= GOOGLEFINANCE("Currency : USDBRL"; "Average") \quad (4.1)$$

- A planilha foi projetada para que, caso o professor opte em usá-la em aula, que os alunos devam alterar somente os campos em cor verde.
- Para realizar um cálculo preciso do consumo do RIG, obtendo assim o consumo energético mensal, foi utilizada a seguinte fórmula:

$$= (B9 * B12 + \$M\$11) * \$L\$21 * \$L\$11 \quad (4.2)$$

Sendo assim, caso a planilha não seja usada pelos alunos, pode-se recomendar a pesquisa da taxa de câmbio no momento da aula, daí basta multiplicar a valor encontrado pela calcula pela taxa encontrada.

- Para a pesquisa em marketplaces, recomendam-se lojas de varejo já conhecidas pelas comunidades de tecnologia. Bons exemplos são como kabum.com, terabyteshop.com e aliexpress.com¹³ e entre outros.

¹³ Por se tratar de uma loja internacional, para esta entrada em específico pode-se incentivar os alunos a considerarem uma chance de taxação, sendo 60% do valor declarado do produto como imposto devido a fiscalização da Receita Federal Brasileira (RFB). Leia mais sobre isto em (OLIVEIRA, 2021)

4.4 Exemplo de plano de aula

Colégio Estadual Minerador Satoshi Nakamoto	
Projeto de intervenção com <i>hands-on</i> : Mineração, vale a pena investir?	
Disciplina	Matemática
Turma	902
Alunos	21
Ano	9ºano
Tempo de aula	100 minutos
Tema da atividade	Nesta atividade vamos estudar o tempo de recuperação de investimentos em um RIG de mineração, tomando como base os cálculos realizados em uma calculadora de lucros.
Objetivo	Perfilhar novas concepções na matemática financeira, exibindo e simulando uma situação por meio de pesquisa temática. Instar a compreensão da matemática dentro do escopo proposto, tornando significativo sua aplicação e desenvolvimento.
Conteúdo	Para os alunos nenhum conteúdo fora do escopo escolar é mandatório para esta atividade, necessitando somente do acompanhamento das atividades previamente realizadas em sala de aula. Recomenda-se que o professor já tenha ministrado aulas anteriores com escopo de finanças.
Referências	BNCC.EF09MA18, BNCC.EF08MA04, BNCC.EF05MA19,

Tabela 5 – Exemplo de plano de aula

4.4.1 Materiais necessários e opcionais

- Acesso a internet (obrigatório)
- Acesso a hardware com acesso a internet (obrigatório)
- Acesso a softwares para ferramentas de pesquisa (obrigatório)
- Acesso ao demonstrativo de gastos na energia elétrica da residência do aluno (obrigatório)
- Disponibilidade de software de edição de planilhas como o *Microsoft Excel*, *Google Sheets* ou *Libreoffice Calc* (opcional)

4.4.2 Metodologia

1. Reservar com a coordenação da escola ou departamento apropriado um horário no laboratório de informática.

Nota importante: É de todo oportuno trazer à baila que, constatando a impossibilidade de comparecimento ao espaço de do laboratório, outrora por mau funcionamento do equipamento fornecido ou impedimento independente, recomenda-se que o docente aplicador tenha equipamento próprio como um projetor. Outrossim, adaptando a metodologia, manter os alunos em sala de aula, e seguir dali conforme metodologia, apresentando em slides a exibição dos dados e websites aqui propostos. A fim de corroborar com o prevalecimento da ordem pública, fica vetado em primeira mão para objeto de desvio de atenção o uso de celulares ,além do uso de redes sociais.

2. No dia e horários reservados, o professor deve entrar em sala, realizar a presença dos alunos, transmitir informações e avisos necessários. Em seguida, antes de acessar os equipamentos, coletar os demonstrativos de gastos na energia elétrica da residência dos alunos¹⁴, em seguida calcular com os alunos a valor cobrado do kilowatt pela companhia energética¹⁵. Orientar os alunos na utilização da planilha fornecida, ou incentivá-los a construir algo semelhante a planilha piloto¹⁶ de cálculo de retorno de investimentos por meio da aplicação de edição de planilhas.
3. Em seguida, orientá-los a acessarem seus navegadores e direcioná-los para a ferramenta de pesquisa favorita. Seguir a atividade incitando a pesquisa de modelos de

¹⁴ Se os alunos forem todos do mesmo município, supondo uma aula presencial, apenas um dos demonstrativos é suficiente

¹⁵ Veja mais na seção guia do professor em 4.3

¹⁶ Conforme também supracitado no guia do professor, há um link para download da planilha piloto no apêndice deste documento. (5.2)

GPUs, pesquisarem em Marketplaces os valores médios de compra destes componentes e em seguir utilizar a calculadora de lucros para obter o rendimento de uma GPU por dia, além de seu consumo energético. No exemplo, podemos ver as variações nas mais diversas moedas como ETH, RVN, FIRO e muitas outras. Como queremos

Figura 15 – Lista de lucratividade média diária de criptomoedas

Name(Tag) Algorithm	Block Time Last Block	Block Reward	Difficulty NetHash	Est. Rewards Est. Rewards 24h	Exchange Rate	Market Cap Volume	Rev. BTC Rev. 24h	Rev. \$ Profit	Profitability Current 24h 3 days 7 days
 Ycash(YEC) EquihashZero	BF: 2m 29s BR: 5.94 LB: 1,042,869	435.600 23.95 kh/s 6.9%	4.7089 5.0329	0.00000735 (Hotbit) 9.8%	\$5,267,101 0.40 BTC	0.000035 0.000037	\$2.26 \$2.26	94% 105% 102% 102%	
 Ethereum(ETH) Ethash ①	BF: 13.54s BR: 2.19 ① LB: 13,468,623	9,660,454,232M 713.42 Th/s -1.7%	0.0006 0.0005	0.06496900 (Binance) -0.5%	\$469,603,932,040 7,368.77 BTC	0.000037 0.000035	\$2.17 \$2.17	100% 100% 100% 100%	
 Firo(FIRO) MTP	BF: 4m 33s BR: 6.25 LB: 418,182	1,233.041 19.40 Gh/s 0.5%	0.2549 0.2563	0.00013490 (Binance) -2.2%	\$102,744,618 25.43 BTC	0.000034 0.000035	\$2.12 \$2.12	93% 98% 99% 97%	
 Nicehash-Ethash Ethash ①	BF: - BR: - LB: -	- 53.51 Th/s -1.0%	0.000034 0.000034	1.23325816 (Nicehash) 1.6%	- 65.50 BTC	0.000034 0.000034	\$2.07 \$2.07	93% 96% 92% 92%	
 Swap(XWP) Cuckaroo29s	BF: 14.82s BR: 1.01 LB: 6,158,211	8,832 595.00 h/s 24.9%	54.9789 68.5781	0.00000048 (TradeOgre) 16.6%	\$417,311 0.02 BTC	0.000026 0.000033	\$2.02 \$2.02	71% 93% 93% 90%	
 Flux(FLUX) ZelHash	BF: 2m BR: 37.50 LB: 974,847	3,305.116 225.63 kh/s 0.3%	5.2979 ① 5.3125 ①	0.00000599 (Gate.io) 7.8%	\$79,717,692 4.04 BTC	0.000032 0.000032	\$1.95 \$1.95	86% 90% 86% 82%	
 BitTubeCash(TUBE) CuckooCycle	BF: 15.07s BR: 8.20 LB: 2,581,701	10,360 687.00 h/s -1.4%	353.8921 ① 348.9943 ①	0.00000009 (Bittrex) 4.2%	\$1,790,759 0.04 BTC	0.000032 0.000031	\$1.92 \$1.92	86% 89% 87% 84%	
 Tent(TENT) Zhash	BF: 1m BR: 6.00 LB: 1,996,461	36.073 4.93 kh/s -11.6%	102.2758 90.5548	0.00000033 (Stex) 6.5%	\$781,377 0.00 BTC	0.000034 0.000030	\$1.83 \$1.83	91% 84% 80% 78%	
 Zclassic(ZCL) EquihashZero	BF: 1m 15s BR: 0.78 LB: 1,349,045	23.598 2.58 kh/s -0.6%	11.3088 11.2423	0.00000262 (Hotbit) 0.7%	\$1,490,082 0.01 BTC	0.000030 0.000029	\$1.80 \$1.80	80% 83% 79% 72%	

Fonte: (WHATMINE, 2020)

- Em seguida, deve-se calcular a conversão de câmbio entre BRL e USD, e consequentemente multiplicar tais valores para uma base de cálculo mensal. Daqui subtrai-se o consumo energético e pode-se ter uma ideia de quantos meses são necessários para que os lucros obtidos integralizem o investimento feito inicialmente.

4.4.3 Avaliação

Ao fim da aula, deve ser observado se os alunos tiveram as capacidades de acompanhar as atividades propostas corretamente, além da participação, e trabalho em grupo. Relevar se surgirem problemas ao tempo de aula, ou se os materiais se tornarem escassos (falhas de *hardware*, interrupções por queda de energia, fenômenos da natureza)

4.5 Exemplo de resultado

Figura 16 – Planilha de cálculo de lucros, parte 1

			
Modelo de GPU	GTX1070Ti	RX 6700	RTX3070
Consumo em W	120	110	130
Consumo em kW	0,12	0,11	0,13
Preço por GPU	R\$ 3.500,00	R\$ 5.500,00	R\$ 7.000,00
Unidades de GPU	6	6	6
Preço total GPUs + RIG	R\$ 26.000,00	R\$ 38.000,00	R\$ 47.000,00
Rendimento por GPU/dia (\$USD)	\$ 2,19	\$ 3,79	\$ 4,59
Rendimento diário (\$USD)	\$ 12,90	\$ 22,74	\$ 27,54
Rendimento diário (R\$ BRL)	R\$ 73,52	R\$ 129,60	R\$ 156,96
Rendimento mensais (R\$ BRL)	R\$ 2.205,67	R\$ 3.888,13	R\$ 4.708,84
Consumo energético mensal	\$ 563,76	\$ 524,88	\$ 602,64
Lucro líquido mensal (R\$ BRL)	R\$ 1.641,91	R\$ 3.363,25	R\$ 4.106,20
% do investimento	6,32%	8,85%	8,74%
Tempo retorno investimento(Meses)	15,84	11,30	11,45

Fonte: Desenvolvido pelo autor com software de manipulação de planilhas

Figura 17 – Planilha de cálculo de lucros, parte 2

		
GPU 05	Custo do RIG	
	R\$ 5.000,00	
	Tarifa de Energia (BRL/kWh) Fator de consumo RIG	
	R\$ 0,90	0,5
R\$ 5.000,00	Dias de trabalho mensal	
\$ -	30	
R\$ -		
R\$ -		
\$ 97,20	Horas de trabalho mensal	
-R\$ 97,20	720	
-1,94%	Cotação \$USD - R\$BRL	
	5,7003	
	-51,44	

Fonte: Desenvolvido pelo autor com software de manipulação de planilhas

Nas figuras acima, usando a planilha piloto foram realizadas três simulações com parâmetros com GPUs existentes no banco de modelos em (WHATTOMINE, 2020), com uma taxa de energia aferida de uma conta de gasto energético real. Após os cálculos obtiveram-se, respectivamente, 15,84 , 11,30 e 11,45 meses para o retorno de um investimento. Retornando ao questionamento feito em 4.1.1, um motorista conseguiria liquidar todo seu investimento neste tempo encontrado? Fica para o leitor responder a esta pergunta.

Capítulo 5

Considerações Finais

*“Invista seu dinheiro no comércio exterior, e
um dia desses você terá lucro.” -
Ecclesiastes 11:1, Good News Bible (GNB)¹.
(tradução livre)*

Neste último capítulo buscou-se trazer os resultados obtidos tomando nota os objetivos gerais e específicos. Tem-se que os resultados aqui obtidos podem ser classificados como satisfatórios, de tal forma que todos os objetivos estabelecidos foram devidamente cumpridos. Abaixo, algumas rápidas considerações.

5.1 Conclusões

A tecnologia traz seus avanços a cada dia que sucede e estes vêm se tornando ferramentas cada vez mais indispensáveis. Um exemplo seria o acesso ao sistema interglobal de redes computadorizadas². Por causa disto, há entre vós muitos artefatos que se moldaram devido ao seu surgimento e muitos outros que só puderam existir devido a sua concepção.

O presente instrumento procurou trazer de forma simplificada que as criptomoedas são um exemplo destes artefatos que só puderam existir e permanecer aos dias atuais devido a conectividade global, além de toda a história que antecedeu todo este processo.

A evolução das moedas nos mostrou que estas perduraram por um grande número de formas ao decorrer da história, desde o escambo aos preciosos metais pesados até a moeda

¹ Citação original do inglês: “Invest your money in foreign trade, and one of these days you will make a profit.” (BÍBLIA SAGRADA (GNB), 1966)

² Popularmente conhecida como internet

impressa, e finalmente aos cartões de crédito e débito até aos criptoativos, sempre se modelando para satisfazer às necessidades da expansão da sociedade, e claro, sempre buscando a aceitação do coletivo, desempenhando suas múltiplas funções³.

Muitas destas mudanças foram proporcionadas pelo desenvolvimento tecnológico, e se tratando de segurança, a tecnologia de registro blockchain surgiu como base e solução como um banco de dados seguro e de registros imutáveis, tudo isso graças a internet e sua base de usuários. Nesta tecnologia já é utilizada por centenas de empresas e avanços significativos em possíveis implementações é esperada.

E ainda tem mais, propomos e desenvolvemos uma atividade usando os conceitos de mineração para calcular as taxas de retorno de um investimento físico para desenvolver estes recursos.

5.2 Trabalhos futuros

Tomando então como concluídos os desafios e objetivos aqui propostos tendo em vista os resultados aqui obtidos, sugere-se que em trabalhos posteriores a este:

- Sejam atualizadas todas as definições sobre a aceitação das criptomoedas no mundo, indicando o surgimento de novas melhorias no sistemas utilizados, se existerem novas criptomoedas relevantes para o cenário econômico mundial e se algumas delas caíram em desuso.
- Desenvolver e relatar novas propostas para o aumento da literacia em criptoativos em meio as populações mundiais, utilizando a proposta de pesquisa aqui disposta para definir novos censos neste tema, medindo e comparando os dados dispostos atuais com os dados obtidos futuramente.
- Retratar sobre as consequências que a baixa literacia em criptoativos já tem causado na população geral, sendo propensa a atuação de criminosos causando prejuízos por meio da aplicação de golpes com esse tema, resultando em valores transferidos de forma fraudulenta para suas carteiras.

³ Suas funções são estas:

I Servir como meio de troca

II Atuar como unidade

III Criar reservas de valor

Referências Bibliográficas

7GRAUS. *Numismática - Dicio, Dicionário Online de Português*. 2011. Acesso em: 02 de dezembro de 2021. Disponível em: <<https://www.dicio.com.br/numismatica>>. Citado na página 24.

AGÊNCIA DINO. *99% dos brasileiros não conseguem passar em uma avaliação de conhecimento básico de criptomoedas*. 2021. Acesso em: 02 de novembro de 2021. Disponível em: <<http://www.broadcast.com.br/cadernos/releases/?id=YStWbG8rNHI1MGhzRG5TZ1p2RXJUQT09>>. Citado na página 38.

BANCO CENTRAL DO BRASIL. *CIRCULAR Nº 3.115 de 23 /04 /2002*. 2002. Acesso em: 25 de dezembro de 2021. Disponível em: <https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/46887/Circ_3115_v5_P.pdf>. Citado na página 31.

BANK OF CANADA. *A History of the Canadian Dollar - New France*. 2019. Disponível em: <<https://www.bankofcanada.ca/wp-content/uploads/2010/07/1600-1770.pdf>>. Citado na página 28.

BARCELLOS, T. *Banco Central prepara moeda virtual para 2022*. 2021. Acesso em: 13 de dezembro de 2021. Disponível em: <<https://economia.uol.com.br/noticias/estadao-conteudo/2021/12/05/banco-central-prepara-moeda-virtual-para-2022.htm>>. Citado na página 37.

BEZERRA, J. *Mercantilismo*. 2020. Disponível em: <<https://www.todamateria.com.br/mercantilismo/>>. Citado na página 29.

BRASIL, J. *Câmara dos Deputados aprova lei para regulamentar criptomoedas no Brasil*. 2021. Acesso em: 11 de dezembro de 2021. Disponível em: <<https://www.jb.com.br/economia/criptomoedas/2021/12/1034557-camara-dos-deputados-aprova-lei-para-regulamentar-criptomoedas-no-brasil.html>>. Citado na página 37.

BROWN, A. *The Poker Face of Wall Street*. Wiley, 2011. Acesso em: 25 de dezembro de 2021. Disponível em: <[https://ztcprep.com/library/Cryptocurrency/The_Poker_Face_of_Wall_Street/The_Poker_Face_of_Wall_Street_\(www.ztcprep.com\).pdf](https://ztcprep.com/library/Cryptocurrency/The_Poker_Face_of_Wall_Street/The_Poker_Face_of_Wall_Street_(www.ztcprep.com).pdf)>. Citado na página 21.

BÍBLIA SAGRADA (ACF). Edição almeida corrigida fiel. Português, 1994. Citado na página 22.

BÍBLIA SAGRADA (GNB). Good news bible. Inglês, 1966. Citado na página 56.

CANALTECH. *A empresa Paypal*. 2020. Acesso em: 19 de dezembro de 2021. Disponível em: <<https://canaltech.com.br/empresa/paypal/>>. Citado na página 31.

COINBASE. *Preço de Bitcoin*. 2021. Acesso em: 13 de julho de 2021. Disponível em: <<https://www.coinbase.com/pt/price/bitcoin>>. Citado na página 18.

CUNHA, C. *Medidas antigas e presentes*. 2011. Acesso em: 20 de dezembro de 2021. Disponível em: <<https://www.programacaopressiva.net/2012/08/computacao-distribuida-introducao-e.html>>. Citado na página 44.

DOMINA CONCURSOS. *Os Bancos Na Era Digital*. 2021. Acesso em: 28 de dezembro de 2021. Disponível em: <<https://pt.scribd.com/document/523085562/01-Os-bancos-na-Era-Digital>>. Citado na página 31.

FRANKENFIELD, J. *Proof of Work (PoW)*. 2021. Acesso em: 12 de dezembro de 2021. Disponível em: <<https://www.investopedia.com/terms/p/proof-work.asp>>. Citado na página 36.

GARROD, C. *Why is Crypto so important and should I care?* 2018. Acesso em: 24 de julho de 2021. Disponível em: <<https://www.conyers.com/publications/view/why-is-crypto-so-important-and-should-i-care/>>. Citado na página 18.

GOLDBERG, D. Famous myths of "fiat money". *Journal of Money, Credit and Banking.*, 0, p. 957–967, 2005. Citado na página 22.

GRENVILLE, D.; SELLWOOD, J. *Coinage In Western Continental Europe, Africa, And The Byzantine Empire*. 2019. Disponível em: <<https://www.britannica.com/topic/coin/Charlemagne-and-the-Carolingian-coinages>>. Citado na página 27.

HUMPHREY, J. W.; OLESON, J. P.; SHERWOOD, A. N. Greek and roman technology. *Routledge*, 0, p. 487, 1997. Citado na página 25.

KENTON, W. *IOU*. 2021. Acesso em: 28 de dezembro de 2021. Disponível em: <<https://www.investopedia.com/terms/i/iou.asp>>. Citado na página 28.

KEYNES, J. M. The general theory of employment, interest and money. Book VI - Short Notes Suggested by the General Theory, p. 5, 1936. Citado na página 29.

KIEPERT, H. *Lycaonia. Asia citerior*. 2013. Disponível em: <https://pt.wikipedia.org/wiki/L%C3%A1ndia#/media/Ficheiro:Heinrich_Kiepert._Asia_citerior.Lydia.jpg>. Citado na página 27.

KRUGMAN, P. R. *The International Role of the Dollar: Theory and Prospect*. National Bureau of Economic Research, Inc: [s.n.], 1984. Acesso em: 30 de junho de 2021. Disponível em: <<http://ideas.repec.org/h/nbr/nberch/6838.html>>. Citado na página 22.

LEGER, J. *Um olhar sobre os Sistemas Imperial e de Unidades Usuais dos EUA de Pesos e Medidas*. 2019. Acesso em: 17 de dezembro de 2021. Disponível em: <https://www.convert-me.com/pt/Imperial_and_US_Customary_Systems_Of_Weights_And_Measures.html>. Citado na página 44.

MINERSTAT OÜ. *Crypto Mining Monitor and Management Software*. 2021. Acesso em: 28 de setembro de 2021. Disponível em: <<https://minerstat.com>>. Citado 2 vezes nas páginas 48 e 49.

MISES, L. V. *The Theory of Money and Credit*. Ludwig von Mises Institute: [s.n.], 1912. Acesso em: 30 de junho de 2021. Disponível em: <<http://mises.org/resources/194>>. Citado na página 22.

MONTEREY, C. *The Oldest Coin in the World*. 2021. Acesso em: 05 de novembro de 2021. Disponível em: <<https://www.montereycompany.com/the-oldest-coin-in-the-world/>>. Citado na página 26.

NAKAMOTO, S. Bitcoin: A peer-to-peer electronic cash system. 2008. Disponível em: <<https://bitcoin.org/bitcoin.pdf>>. Citado na página 36.

NATIONAL GEOGRAPHIC. *Grandes reportagens: as primeiras moedas da historia*. 2020. Disponível em: <<https://nationalgeographic.pt/historia/grandes-reportagens/2099-as-primeiras-moedas-da-historia>>. Citado na página 26.

NELSON, E. *The world's first ATM was installed this week in 1967. Are the cash machine's days numbered?* 2018. Acesso em: 19 de dezembro de 2021. Disponível em: <<https://qz.com/1316814/the-worlds-first-atm-was-installed-this-week-in-1967-are-its-days-numbered/>>. Citado na página 30.

NICEHASH. *Leading Cryptocurrency Platform*. 2021. Acesso em: 14 de julho de 2021. Disponível em: <<https://www.nicehash.com>>. Citado 2 vezes nas páginas 48 e 49.

NPARTNERS. *A questão legal da utilização de criptomoedas no Brasil*. 2021. Acesso em: 10 de dezembro de 2021. Disponível em: <<https://nplaw.com.br/criptomoedas-legislacao-brasil/>>. Citado na página 37.

OCDE. *Recommendation on Principles and Good Practices For Financial Education and Awareness*. 2005. Acesso em: 15 de junho de 2021. Disponível em: <<https://www.oecd.org/finance/financial-education/35108560.pdf>>. Citado na página 44.

OLIVEIRA, R. *Como funciona a taxação de produtos importados*. 2021. Acesso em: 25 de dezembro de 2021. Disponível em: <<https://www.promobit.com.br/blog/como-funciona-a-taxacao-de-produtos-importados-297>>. Citado na página 50.

ORTON, L. Financial literacy: Lessons from international experience. Canadian Policy Research Network - CPRN Research Report., 2017. Citado na página 44.

OXFORD UNIVERSITY PRESS. *Oxford Learners Dictionary*. 2021. Acesso em: 22 de junho de 2021. Disponível em: <<https://www.oxfordlearnersdictionaries.com/us/definition/english/cryptography>>. Citado na página 32.

PEIXOTO, F. BBC - Ministros do G20 discutem 'guerra cambial'. 2010. Acesso em: 25 de novembro de 2021. Disponível em: <https://www.bbc.com/portuguese/noticias/2010/10/101008_entenda_guerra_cambial>. Citado na página 28.

PRIBERAM. *Cunhagem - Dicionário Online Priberam de Português*. 2021. Acesso em: 02 de dezembro de 2021. Disponível em: <<https://dicionario.priberam.org/cunhagem>>. Citado na página 25.

PROGRAMAÇÃO PROGRESSIVA. *Computação Distribuída: Introdução e exemplos de uso*. 2021. Acesso em: 02 de outubro de 2021. Disponível em: <<https://www.programacaoprogressiva.net/2012/08/computacao-distribuida-introducao-e.html>>. Citado na página 33.

RETRWORKS. *Caesar Cipher Medallion Original Retroworks*. 2021. Acesso em: 04 de dezembro de 2021. Disponível em: <<https://www.amazon.com/Retroworks-Classic-Caesar-Medallion-Decoder/dp/B004D1L0B0>>. Citado na página 34.

RIVEST, R. L. Handbook of theoretical computer science. "Criptografia", em J. Van Leeuwen (ed.). *Handbook of Theoretical Computer Science*, 1990. Citado na página 32.

SANBORN, J. *Notes about Kryptos and Cyrillic Project*. 2003. Acesso em: 25 de dezembro de 2021. Disponível em: <<https://mathweb.ucsd.edu/~crypto/Projects/IrinaDubova/Mynotes.htm>>. Citado na página 32.

SHIEBER, J. *Fidelity CEO Abigail Johnson says the company is mining cryptocurrencies*. 2017. Acesso em: 25 de dezembro de 2021. Disponível em: <<https://techcrunch.com/2017/09/28/fidelity-ceo-abigail-johnson-says-the-company-is-mining-cryptocurrencies/>>. Citado na página 42.

TEXAS REPUBLIC BANK. *Origin of Paper Money*. 2019. Acesso em: 28 de dezembro de 2021. Disponível em: <<https://texaspublicbank.com/origin-of-paper-money/>>. Citado na página 28.

THE BITCOIN PROJECT. *Bitcoin - Open source P2P money*. 2021. Acesso em: 11 de dezembro de 2021. Disponível em: <<https://bitcoin.org/en/faq>>. Citado na página 36.

TIKKANEN, A. *A Brief (and Fascinating) History of Money*. 2020. Disponível em: <<https://www.britannica.com/story/a-brief-and-fascinating-history-of-money>>. Citado 3 vezes nas páginas 23, 27 e 29.

TOLOTTI, R. *B3 detalha planos para custódia de criptomoedas, tokenização e ETF de cripto em 2022*. 2021. Acesso em: 15 de dezembro de 2021. Disponível em: <<https://www.infomoney.com.br/mercados/b3-detalha-planos-para-custodia-de-criptomoedas-tokenizacao-e-etf-de-cripto-em-2022/>>. Citado na página 37.

WHATMINE. *Crypto coins mining profit calculator*. 2020. Acesso em: 30 de setembro de 2021. Disponível em: <<https://www.whattomine.com>>. Citado 6 vezes nas páginas 42, 47, 48, 49, 53 e 55.

WHIMSICAL. *Where Great Ideas Take Shape*. 2021. Acesso em: 21 de setembro de 2021. Disponível em: <<https://www.whimsical.com>>. Citado 5 vezes nas páginas 23, 24, 31, 35 e 73.

YU, L.; YU, H. Chinese coins: Money in history and society. Long River Press, 2004. Citado na página 25.

Apêndice

APÊNDICE A - Planilha de cálculo de retorno de investimentos.

- Link 1 - Principal
<https://bit.ly/3DZpKD>
- Link 2 - Backup e sem restrições de alterações
<https://bit.ly/3F2rkWA>

APÊNDICE B - Formulário de pesquisa temática distribuído para os participantes sem acesso a internet (inicia na próxima página).

Dos primeiros meios de pagamento aos criptoativos, uma breve síntese para alunos dos ensino fundamental e médio

-----Português do Brasil abaixo-----

Prezado participante,

Obrigado pelo seu interesse em participar desta pesquisa. A seguir voce participará do preenchimento deste formulário para contribuir com o desenvolvimento do TCC (sob o tema deste formulário) de Lucas Herick Silva, graduando em Matemática pela Universidade Federal Fluminense, Rio de Janeiro, Brasil. Este formulário é direcionado a homens e mulheres maiores de 18 anos brasileiros ou estrangeiros. Ter uma carteira de investimentos em criptoativos, ativos em bolsa de valores ou formação superior não são um pre-requisito. O preenchimento deste questionário deve levar em média 10 minutos.

Este questionário será apresentado em português brasileiro(PT-BR) a partir desta página. Se você não tem familiaridade com o português brasileiro, você tem permissão (e encorajamento) a usar ferramentas de tradução automática para esta pesquisa, como o Google Tradutor.

Seu nome e dados aqui fornecidos estarão sob sigilo e serão analisadas junto com as informações dos outros participantes, sem que haja exposição da identidade de cada participante.

-----US English below-----

Dear participant,

Thank you for your interest in participating this survey. Next, you will be participating in the completion of this form to contribute to the development of the final undergraduate thesis by Lucas Herick Silva (www.airherick.com), currently pursuing a degree in Mathematics at Fluminense Federal University in Rio de Janeiro, Brazil. This form is intended for brazilian and foreigners, man and woman over 18 years old. Having an investment portfolio in cryptoactives, stock markets or pursue higher education is not a pre-requisite. Completing this questionnaire should take an average of 10 minutes.

This questionnaire will be taken in Brazilian portuguese (PT-BR) beyond this page. You are allowed (and incentivated) to use automated translator tools for this research such as Google Translator.

Your name and data provided here will be confidential and will be analyzed together with the information of other participants, without exposing the identity of each participant.

*Required

**Termo de Consentimento
Livre e Esclarecido**

Undergraduate thesis personality quiz: From the first payment methods to cryptocoins

Antes de começar com a pesquisa, por favor, leia atentamente o Termo de Consentimento Livre e Esclarecido do Pesquisado. Após sua confirmação, será possível dar início à pesquisa.

Termo de Consentimento Livre e Esclarecido

O (A) Sr. (a) está sendo convidado(a) a participar da pesquisa "Dos meios de pagamento aos criptoativos, uma breve síntese para alunos dos ensino fundamental e médio." conduzido por Lucas Herick Silva.

A presente pesquisa visa obter uma maior compreensão acerca dos perfis de consumidores tanto Brasileiros quanto internacionais (se aplicar) sobre seu conhecimento geral sobre criptoativos. A próxima página dará acesso ao questionário online, mas para confirmar sua participação é preciso que você leia abaixo algumas considerações importantes:

1. O experimento é composto de uma única sessão experimental durando cerca de 5 a 10 minutos. Esta sessão será realizada via online por meio do computador, celular, ou outro aparelho eletrônico que tenha disponível no local onde se encontra e que permita acessar o Google Forms. Durante o experimento você irá preencher uma série de perguntas a respeito dos seus conhecimentos gerais sobre investimentos em criptoativos, além de percepções gerais sobre o tema.
2. Esta pesquisa será liderada por Lucas Herick Silva, que é graduando em matemática pela Universidade Federal Fluminense.
3. Lembre-se que em qualquer etapa da pesquisa você está livre para abandonar o experimento e retirar o seu termo de consentimento, sem qualquer prejuízo, caso se sinta incomodado com qualquer aspecto do teste.
4. Concordando em participar, por favor, pedimos que preencha todos os itens para que seja possível analisar os dados de maneira precisa.

Agradecemos por sua contribuição!

1. Você concorda em participar desta pesquisa? *

Mark only one oval.

- Concordo com os termos acima e concordo em participar
 Não concordo com os termos acima

**Setor demográfico
(1 de 4)**

Esta seção será responsável por mapear demograficamente as respostas dos participantes

2. Qual o teu nome e sobrenome? (Lembrando que suas respostas não serão usadas para lhe identificar, o teor desta questão serve somente para eliminar respostas duplicadas) *

3. Qual o teu sexo? *

Mark only one oval.

- Masculino
- Feminino
- Prefiro não dizer

4. Em qual opção melhor encaixa tua idade? *

Mark only one oval.

- Menor de 18 anos
- 18 anos a 24 anos
- 25 anos a 34 anos
- 35 anos a 44 anos
- 45 anos a 54 anos
- Maior que 54 anos

5. Em qual nível acadêmico você está cursando ou já concluiu? *

Mark only one oval.

- Ensino fundamental
- Ensino médio
- Graduação (Undergraduate)
- Mestrado ou MBA
- Doutorado

6. Quais é o teu background acadêmico? (área de estudo, se houver) *

Mark only one oval.

- Matemática/Estatística
- Tecnologia da Informação ou correlato
- Não possuo
- Other: _____

7. Qual o teu estado civil? *

Mark only one oval.

- Solteiro
- Casado
- Divorciado
- Viúvo
- Tá complicado (°_°)

8. Em relação ao teu trabalho/estudo, selecione aquele que melhor se aplica *

Mark only one oval.

- Trabalho de meio tempo e não estudo (20+ horas)
- Trabalho de tempo integral e não estudo (40+ horas)
- Desempregado
- Estudante integral (full-time, 40+ horas)
- Aposentado
- Estudante de meio tempo, trabalho de meio tempo ou integral (60+ horas)
- Dupla jornada (Trabalho e estudo ambos de tempo integral, 80 horas)

9. Com quais idiomas voce tem familiaridade? Marque todas as opções que melhor se aplicam

Tick all that apply.

- Português
- Inglês
- Coreano
- Espanhol
- Italiano
- Francês
- Alemão
- Japonês
- Chinês

Other: _____

Setor de Perfilamento (2 de 4)

10. Pare, feche os teus olhos e pense na palavra DINHEIRO. Quais as duas primeiras imagens que vem a tua cabeça? *

11. Você possui um orçamento doméstico? Pense num orçamento doméstico como um papel ou planilha de controle de gastos *

Mark only one oval.

- Sim!
- Não, eu não tenho tempo pra isso
- Não, eu não sei por onde começar
- Não, eu não ganho o suficiente pra isso
- Não, eu não preciso de um orçamento
- Não sei

12. Dado o seu orçamento mensal, você consegue ficar dentro dele? *

Mark only one oval.

- Maioria das vezes
- Sempre
- Nunca
- As vezes
- Não sei
- Raramente

13. Suponha que sobraram algumas centenas de reais no orçamento. Onde você mantém/investe este dinheiro? Selecione aqueles que melhor se aplicam *

Tick all that apply.

- Bolsa de valores
- Criptoativos
- Dentro do colchão ou cofre caseiro
- Arranjaria novas despesas para gastar
- Fundo monetário
- Compraria ouro
- Compraria dólares ou euros (câmbio)
- Poupança
- Não sei

14. Você possui dinheiro investido hoje? Onde? Selecione aqueles que melhor se aplicam *

Tick all that apply.

- Bolsa de valores
- Criptoativos
- Fundo monetário
- Ouro
- Câmbio
- Poupança
- Não sei
- Não possuo dinheiro investido

15. Você está se preparando financeiramente para sua aposentadoria? *

Mark only one oval.

- Sim
- Não
- Já sou aposentado
- Não sei

16. O quanto você acha que conhece sobre criptoativos? *

Mark only one oval.

- Nunca ouvi falar *Skip to question 24*
- Conheço só os nomes
- Muito pouco
- Um pouco
- Moderadamente
- Muito

17. Você planeja comprar ou vender criptomoedas nos próximos 6 meses? *

Mark only one oval.

- Sim
- Não
- Talvez

18. Se você respondeu sim ou talvez acima, porque o faria? *

Tick all that apply.

- Respondi "Não" na pergunta acima
- Para guardar para o futuro
- Para comprar bens e serviços
- Para mandar a família ou amigos
- Para obter independência financeira
- Nenhum destes

Other:

**Teste rápido
de
"criptoliteracia"
(3 de 4)**

Neste mini teste o objetivo é estipular a "criptoliteracia" dos participantes. Responda as cinco (5) questões abaixo com a alternativa que você acredita que melhor se aplique.

19. Quais destas frases melhor descreve um criptoativo: *

Mark only one oval.

- Dinheiro que pode ser armazenado fisicamente ou eletronicamente
- Dinheiro em papel que só podem ser usados para transações físicas
- Uma moeda digital ou virtual protegida por criptografia
- Moeda que só pode ser usada para remessas internacionais
- Eu não sei

20. Quais destes você acredita que não seja uma criptomoeda: *

Mark only one oval.

- Ethereum
- Litecoin
- Dogecoin
- Metamask
- Stellar Lumens
- Eu Não sei

21. O que é a mineração de criptomoedas? *

Mark only one oval.

- Uma rede de carteiras físicas e digitais enviando e recebendo ativos digitais entre si
- Mantendo a segurança do blockchain, é o processo que aumenta a quantidade de moedas em circulação.
- Um aplicativo de telefone onde os usuários resolvem ou jogam jogos e recebem criptomoedas como recompensa
- O processo de mineração de metais preciosos para financiar o desenvolvimento de um projeto de criptografia
- Eu não sei

22. Moedas regulamentadas, apoiadas por bancos centrais, tem divisibilidade limitada. Um real, por exemplo, só pode ser dividido em 100 partes de centavo, cada uma valendo R\$ 0,01. Quantas unidades, ou casas decimais, um bitcoin pode ser dividido? *

Mark only one oval.

- 3 casas decimais
- 8 casas decimais
- 20 casas decimais
- Nenhum. Você não pode dividir um bitcoin em um decimal
- Eu não sei

23. Qual métrica é usada para medir o poder de processamento de uma rede de mineração de criptomoedas? *

Mark only one oval.

- CPUs
- Hashrates (h/s)
- Megahertz (MHz)
- Gigahertz (GHz)
- Eu Não sei

**Final
(4
de
4)**

Chegamos ao fim da pesquisa, esta é a última pergunta! Muito obrigado pela sua participação! Se você quer dizer algo a mais, como elogios, críticas construtivas ou ideias para novos questionamentos esta é sua última chance! Se não, clique no botão enviar no fim da página.

24. Insira aqui elogios, críticas construtivas ou ideias para novos questionamentos, caso tenha :)

This content is neither created nor endorsed by Google.

Google Forms

Glossário

- Asset Assets são conjuntos de objetos disponíveis para desenvolvimento de exemplos de aplicações, imagens, vídeos em diversas plataformas. Especificamente falando do (WHIMSICAL, 2021), os assets são conjuntos de ícones e setas para o desenho de infográficos, mapas mentais e post-its.
- AMD Fabricante de GPUs AMD, cujo nome vem do inglês e significa *Advanced Micro Devices* ou “Micro aparelhos avançados”. É uma empresa multinacional americana de semicondutores com sede em Santa Clara, Califórnia, que desenvolve processadores de computador e outros tipos de hardware.
- Backup Um backup de um certo dado é uma cópia de segurança deste dado, porém obtido e armazenado em outra localização para frutos de restauração em caso de perda do dado original ou acidente
- Ethash Ethash é o algorítmo de mineração oficial para ETH. Trata-se de um algoritmo de alta qualidade que usa elaboradas técnicas computacionais para garantir a maior segurança possível na mineração.
- Ethash4G Ethash4G é uma derivação do ethash e permite que GPUs com 4GB de VRAM consigam minerar.
- Fintech Junção das palavras financial e technology (financeiro e tecnologia) do inglês. São startups nos quais o uso da tecnologia é o principal diferencial, se comparados com outras empresas do mesmo ramo. Desenvolvem produtos financeiros totalmente digitais.
- Frame Os Frames são gabinetes especializados para mineração e são compostos por estrutura metálicas dando suporte físico para todo hardware de mineração.
- Hands on Trata-se de uma expressão muito utilizada no mundo corporativo que refere-se equivalentemente a expressões do tipo “mão na massa” ou “aprender enquanto se pratica” quando uma demanda ou atividade é aplicada. Também pode significar pró-atividade por parte de um funcionário ou aluno.

Hardware	Conjunto de equipamento físico de qualquer sistema gerenciado computacionalmente. Constituem-se de peças e equipamentos que fazem influenciam na velocidade de processamento e capacidade de armazenamento de um sistema, além de outras funções
Kawpow	Kawpow é o algorítmo de mineração oficial para RVN, que foi implementado em 6 de maio de 2020.
Marketplace	No mundo físico trata-se de um espaço aberto onde um mercado ou feira é ou foi realizado anteriormente em uma cidade. No mundo digital, são páginas programadas e especializadas na compra,venda e troca de objetos.
MTP	MTP (Merkle Tree Proof ou Provas para árvores de Merkle em português) é um algoritmo de mineração PoW usado por Zcoin que mudou para MTP em 10 de dezembro de 2018.
Nvidia	Fabricante de GPUs Nvidia, cujo nome vem da palavra <i>Invidia</i> , do latim, que significa inveja. É uma empresa multinacional americana de tecnologia sediada em Santa Clara, Califórnia que desenvolve GPUs para mercados de jogos e profissionais.
Open-source	Originado na computação, O termo open-source se refere a algo que as pessoas podem modificar e compartilhar pois seu design é acessível ao público.
PySpark	O nome Pyspark se dá pela junção de Python com Apache Spark. Este é considerado uma interface para Apache Spark em Python. Com ele, é possível escrever aplicativos usando APIs Python e é amplamente difundido em grandes empresas por ser open-source.
Rig	Rigs de mineração são o conjunto de sistemas computacionais estruturados para mineração. Este inclui placa-mãe, fonte, memória RAMs, FRAME e RISERs. Sua função é controlar e realizar suporte sobre o processamento realizado por GPUs de alto desempenho.
Riser	Risers são conjunto de cabeamentos elétricos e adaptadores que tem o objetivo de conectar GPUs a outros componentes de um RIG. Tais elementos utilizam um frame para permanecerem em posição.
Software	Conjunto de partes lógicas de qualquer sistema gerenciado computacionalmente. Sua função é executar, realizar instruções e manipular as atividades lógicas por meio de um hardware. Divide-se em softwares de sistemas que permite interações dos usuários e o hardware e software de aplicação, que permitem que o usuário realize

atividades específicas como criação de gráficos, escrita de textos e manipulação de planilhas.

Startup Termo inglês que se traduz como o início de algo novo. São empresas que estão em fase inicial e possuem novos conceitos para mostrar ao mercado.

Índice

- Arquitetura Digital, 46
Avaliação, 38, 53
Bitcoin, 18, 20
Blockchain, 35, 37
BNCC, 45
Bolsa de valores, 37
Calculadoras, 49
Chaves criptográficas
 Chave Assimétrica, 35
 Chave simétrica, 35
Cifra de César, 34
Cloud Computing, 46
Computação distribuída, 33
Criptoativo, 19, 38
Criptografia
 Criptografia, 32
 Criptografia Moderna, 32
Criptomoeda, 18, 37, 43
Cypherpunks, 36
Cálculos em planilha, 49, 54
Câmbio, 50
Divisibilidade, 40
Dogecoin, 39, 43
Educação Financeira, 44
Ethereum, 39, 42, 43, 47, 48
Evolucionários, 20
FIRO, 53
GPU, 47, 49, 53
Hands On, 47
Hardware, 43, 46
Hash, 36, 45
Interdisciplinaridade, 42
Legalidade, 37
Litecoin, 39
Literacia, 44
Marketplace, 50, 53
Metamask, 39
Metodologia, 52
Mineração, 39, 42, 47
Moedas virtuais, 36
Métricas, 41, 44, 45
On Premise, 46
Plano de Aula, 51
Prova de trabalho, 36
Questionário, 38
Ravencoin, 53
Regulamentação, 37
RIG, 47, 49–51
Sistemas Operacionais, 47
Stellar Lumens, 39
Substituição (Criptografia), 33

Tesla, 43

Tranposição (Criptografia), 33

Whattomine, 42, 47–49, 53