UNIVERSIDADE FEDERAL DE CAMPINA GRANDE
Programa de Pós-Graduação em Matemática
Mestrado Profissional - PROFMAT/CCT/UFCG

Émerson Rodrigues Alves

Sequências e Progressões com a cadeia de blocos do *Bitcoin*

Campina Grande - PB
Agosto/2025

UNIVERSIDADE FEDERAL DE CAMPINA GRANDE
Programa de Pós-Graduação em Matemática
Mestrado Profissional - PROFMAT/CCT/UFCG

Émerson Rodrigues Alves

Sequências e Progressões com a cadeia de blocos do *Bitcoin*

Trabalho de Conclusão de Curso apresentado ao Corpo Docente do Programa de Pós-Graduação em Matemática - CCT - UFCG, na modalidade Mestrado Profissional, como requisito parcial para obtenção do título de Mestre.

Orientador: Dra. Deise Mara Barbosa de Almeida
Coorientador: Dr. Leomaques Francisco Silva Bernardo

Campina Grande - PB
Agosto/2025

A474s Alves, Émerson Rodrigues.
Sequências e progressões com a cadeia de blocos do Bitcoin / Émerson Rodrigues Alves. – Campina Grande, 2025.
105 f. : il. color.

Dissertação (Mestrado em Matemática) – Universidade Federal de Campina Grande, Centro de Ciências e Tecnologia, 2025.
"Orientação: Profa. Dra. Deise Mara Barbosa de Almeida, Prof. Dr. Leomaques Francisco Silva Bernardo".
Referências.

1. Matemática – Estudo e Ensino. 2. Sequências e Progressões. 3. Sequências Didáticas. 4. Bitcoin. 5. Blockchain. I. Almeida, Deise Mara Barbosa de. II. Bernardo, Leomaques Francisco Silva. III. Título.

UFCG/BC CDU 51(07)(043.3)

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECÁRIA SEVERINA SUELI DA SILVA OLIVEIRA CRB-15/225

Émerson Rodrigues Alves

Sequências e Progressões com a cadeia de blocos do *Bitcoin*

Trabalho de Conclusão de Curso apresentado ao Corpo Docente do Programa de Pós-Graduação em Matemática - CCT - UFCG, na modalidade Mestrado Profissional, como requisito parcial para obtenção do título de Mestre.

Trabalho aprovado. Campina Grande - PB, 22 de Agosto de 2025.

Documento assinado digitalmente
gov.br
LEOMAQUES FRANCISCO SILVA BERNARDO
Data: 17/09/2025 11:04:28-0300
Verifique em https://validar.iti.gov.br

Dr. Leomaques Francisco Silva Bernardo
Orientador - UFCG

Documento assinado digitalmente
gov.br
RODRIGO COHEN MOTA NEMER
Data: 18/09/2025 17:53:17-0300
Verifique em https://validar.iti.gov.br

Dr. Rodrigo Cohen Mota Nemer
Membro Interno, UFCG

Documento assinado digitalmente
gov.br
PRISCILA SANTOS RAMOS
Data: 19/09/2025 09:32:13-0300
Verifique em https://validar.iti.gov.br

Dra. Priscila Santos Ramos
Membro Externo, UFOB

Campina Grande - PB
Agosto/2025

Dedico este trabalho, primeiramente, a Deus, por me conceder o dom da vida e por iluminar meus caminhos, fortalecendo-me diante dos desafios. Aos meus pais, que mesmo com pouco acesso à educação formal, ensinaram-me valores fundamentais e contribuíram de forma decisiva para minha formação. E ao Satoshi, cuja criação do Bitcoin tornou possível a realização deste trabalho.

Agradecimentos

Aos meus orientadores, Dra. Deise Mara Barbosa de Almeida e Dr. Leomaques Francisco Silva Bernardo, por conduzirem este trabalho com paciência, dedicação e generosidade. Mesmo diante das dificuldades, mantiveram-se sempre dispostos a orientar cada etapa com atenção e cuidado.

À Universidade Federal de Campina Grande (UFCG), por proporcionar este período de aprendizado e desenvolvimento profissional nesse programa PROFMAT/UFCG; aos professores do programa, pelo compromisso com a formação de qualidade; e aos colegas de turma, pela parceria e apoio ao longo da jornada.

Aos meus pais, João Carlos e Maria José, por me educarem com amor, por estarem sempre ao meu lado ao longo da vida e por me apoiarem incondicionalmente em todos os momentos em que mais precisei. Aos meus irmãos, Everton e Luana, por compartilharem comigo tantos momentos bons e ruins ao longo da vida e me apoiarem quando precisei.

À gestão escolar, aos professores e aos alunos da EEFM Reitor Edvaldo do Ó pela valiosa colaboração e pela disponibilidade demonstrada durante o processo de implementação e coleta de dados desta pesquisa.

À minha noiva Ingrid, pelo amor, paciência e incentivo incondicional em cada etapa desta caminhada. Sua presença ao meu lado foi fundamental para que eu pudesse seguir firme, mesmo nos momentos mais desafiadores. Obrigado por acreditar em mim e por ser minha parceira na vida e nos sonhos.

À minha terapeuta Tatiane, pelo apoio essencial que me encorajou a apresentar este tema aos meus orientadores. E a todos que contribuíram, direta ou indiretamente, para a realização deste trabalho.

Bitcoin é uma ferramenta de liberdade; não permita que ele se transforme em sua prisão.

Resumo

O ensino de Matemática desempenha um papel fundamental na formação do pensamento lógico, crítico e na capacidade de resolução de problemas. Este trabalho explora a integração entre conceitos matemáticos de sequências e progressões e a tecnologia *Blockchain* do *Bitcoin*. O objetivo principal é desenvolver uma abordagem didática inovadora que utilize a *Blockchain* como ferramenta para ensinar matemática de forma prática e relevante para os alunos do Ensino Médio. O trabalho aborda a estrutura da *Blockchain*, as sequências numéricas, progressões aritméticas (PA) e progressões geométricas (PG), a sequência de Fibonacci, relacionando-as com o funcionamento do *Bitcoin* e à visualização da cadeia de blocos por meio do site *mempool*. A proposta se concretiza por meio de uma sequência didática que explora os conceitos de sequência numérica, progressões aritméticas e geométricas, associando-os à estrutura da *Blockchain* e ao modelo de política monetária da rede *Bitcoin*. A metodologia envolveu aulas expositivas e atividades práticas, buscando desenvolver habilidades críticas, matemáticas e tecnológicas. Essa dissertação também analisa os dados obtidos a partir de um questionário aplicados aos alunos, avaliando a eficácia da metodologia proposta.

Palavras-chave: Sequências; Progressões; Sequências Didáticas; *Bitcoin*; *Blockchain*.

Abstract

The teaching of Mathematics plays a fundamental role in developing logical thinking, critical reasoning, and problem-solving skills. This work explores the integration between mathematical concepts of sequences and progressions and the blockchain technology of Bitcoin. The main objective is to develop an innovative didactic approach that uses the blockchain as a tool to teach mathematics in a practical and meaningful way for high school students. The study addresses the structure of the blockchain, numerical sequences, arithmetic progressions (AP), geometric progressions (GP), and the Fibonacci sequence, relating them to the functioning of Bitcoin and the visualization of the blockchain through the website mempool.space. The proposal is materialized through a didactic sequence that explores the concepts of numerical sequences, arithmetic and geometric progressions, associating them with the blockchain structure and the monetary policy model of the Bitcoin network. The methodology involved expository lessons and practical activities, aiming to develop critical, mathematical, and technological skills. This dissertation also analyzes data obtained from a questionnaire applied to students, assessing the effectiveness of the proposed methodology.

Keywords: Progressions; Didactic Sequences; *Bitcoin*; *blockchain*.

Lista de ilustrações

Lista de quadros

Sumário

1 Introdução

A matemática, por vezes vista como abstrata e distante da realidade, pode se tornar uma ferramenta poderosa para compreender e interagir com o mundo contemporâneo. Neste contexto, nessa dissertação propomos uma abordagem inovadora para o ensino de sequências e progressões, unindo conceitos matemáticos fundamentais à tecnologia *blockchain* do *Bitcoin*. A escolha do *Bitcoin* como tema central se justifica pela sua crescente relevância no cenário global e pelo seu potencial de despertar o interesse dos alunos. Ao explorar a estrutura da *blockchain*, os alunos são convidados a mergulhar em um universo de sequências numéricas, progressões aritméticas e geométricas, compreendendo como esses conceitos se aplicam na prática.

As sequências e progressões são conceitos da matemática na unidade temática de álgebra e aritmética, representando uma forma organizada de listar números ou termos que seguem uma regra específica. Uma sequência é uma lista ordenada de números, onde cada número é conhecido como um termo. As sequências podem ser classificadas de diversas maneiras, sendo as mais comuns as sequências aritméticas e geométricas. As progressões aritméticas (PA) são aquelas em que a diferença entre termos consecutivos é constante. Por outro lado, as progressões geométricas (PG) caracterizam-se por terem uma razão constante entre termos consecutivos.

Neste trabalho, buscamos promover a integração entre a matemática e a tecnologia contemporânea, utilizando a *blockchain* da rede *Bitcoin* como ferramenta didática. Em um contexto educacional que busca inovar e engajar os alunos, a proposta se destaca ao abordar conceitos matemáticos fundamentais de maneira prática e relevante. Segundo Ulrich (2014), o *bitcoin* é uma moeda digital de ponta a ponta, ou seja, enviada de uma pessoa para outra pessoa sem uma autoridade central para intermediar as transações. De acordo com Nakamoto (2008) o bitcoin utiliza uma cadeia de blocos conhecida como *blockchain*, é uma das inovações mais significativas na tecnologia financeira e de registros digitais. Essa estrutura de dados descentralizada serve como um livro-razão público e imutável, que registra todas as transações realizadas na rede *Bitcoin*.

A cadeia de blocos do *Bitcoin*, conhecida como *blockchain*, é uma tecnologia que registra todas as transações realizadas com a criptomoeda de forma descentralizada. Essa estrutura é composta por uma sequência de blocos, onde cada bloco contém um conjunto de transações, um *timestamp*, o *hash* do bloco anterior e um número chamado nonce, que é utilizado durante o processo de mineração. Cada bloco serve como um registro imutável, garantindo a integridade das informações. Antes que as transações sejam confirmadas e incluídas em um bloco, elas são armazenadas em uma área chamada *mempool*, ou pool de memória. A *mempool* é uma lista temporária de transações que aguardam confirmação, e os mineradores costumam selecionar aquelas com taxas de transação mais altas para incluir no próximo bloco. Essa dinâmica garante que as transações sejam processadas de forma eficiente.

A estrutura da *blockchain* pode ser compreendida através de sequências numéricas, já que cada bloco é adicionado em uma sequência linear, onde a posição de cada bloco depende do bloco anterior. Essa relação não só assegura a integridade da cadeia, mas também a segurança das transações, pois qualquer alteração em um bloco afetaria todos os demais, quebrando a sequência e alertando a rede sobre a manipulação. A proposta metodológica deste trabalho envolve uma sequência didática composta por encontros nos quais os alunos exploram sequências numéricas, incluindo a sequência de Fibonacci, além de progressões aritméticas e geométricas, tudo em um contexto prático e tecnológico, unido à tecnologia *blockchain* do *bitcoin*. A abordagem inclui aulas expositivas, atividades práticas e avaliação formativa, com o objetivo de desenvolver habilidades críticas, matemáticas e tecnológicas.

Este trabalho representa uma oportunidade de integrar a matemática a situações práticas e tecnológicas, preparando os alunos para os desafios do futuro e contribuindo para a melhoria do desempenho acadêmico na disciplina. Ao final do percurso, espera-se que os alunos não apenas compreendam os conceitos de sequências e progressões, mas também sejam capazes de aplicar esses conhecimentos de maneira prática, fortalecendo sua formação acadêmica.

1.1 Objetivos

1.1.0.1 Objetivo Geral

Desenvolver a compreensão dos alunos sobre sequências numéricas, incluindo sequências aritméticas e geométricas, e sua relevância na matemática e na tecnologia.

1.1.0.2 Objetivos Específicos

- Identificar e classificar diferentes tipos de sequências numéricas (finita, infinita, recorrente, não recorrente);
- Introduzir os conceitos básicos da rede Bitcoin e sua importância;
- Explicar a estrutura de blockchain e como a mempool armazena transações em sequência;
- Relacionar a estrutura da blockchain com sequências numéricas e progressões;
- Ensinar a classificar progressões aritméticas e identificar suas características;

- Determinar o termo geral de uma PA e aplicá-lo na análise de recompensas em *Bitcoin*;
- Promover a resolução de problemas práticos que envolvam PA, especialmente em cenários de mineração;
- Introduzir a classificação e o termo geral das progressões geométricas;
- Relacionar PG às recompensas de Bitcoin a cada bloco minerado, demonstrando a aplicação matemática;
- Discutir o conceito do limite total de Bitcoin que pode ser minerado, conectando matemática e tecnologia.

1.2 Organização

Visando ao cumprimento dos objetivos delineados na Seção 1.1, dividimos esta dissertação em 6 capítulos. O Capítulo 1 aborda os aspectos introdutórios e define os objetivos do trabalho. O Capítulo 2 apresenta o embasamento teórico da pesquisa, com foco nos elementos da BNCC. Posteriormente, relacionamos esses conteúdos de sequências e progressões com a estrutura de blocos do *Bitcoin*. O Capítulo 3 é dedicado à apresentação dos conceitos formais, definições e propriedades fundamentais de sequência, progressão aritmética e progressão geométrica. Já no Capítulo 4, descrevemos os fundamentos da rede *Bitcoin*, seu funcionamento e associamos a cadeia de blocos com sequências e progressões. No Capítulo 5, descrevemos um relato de experiência da aplicação da nossa sequência didática sobre o ensino de sequências e progressões com os blocos da rede *Bitcoin* e destacando pontos positivos e negativos na aplicação. Por fim, no Capítulo 6, apresentamos considerações finais e sugestões construtivas com o objetivo de aprimorar o desenvolvimento e a aplicação deste trabalho científico.

2 Referencial Teórico

A Base Nacional Comum Curricular (BNCC) estabelece as diretrizes para o ensino no Brasil e define os conteúdos a serem abordados no ensino médio em relação a sequências e progressões. Essas diretrizes visam garantir que os alunos adquiram as competências necessárias para compreender e aplicar sequências numéricas e seus tipos, como a sequência de Fibonacci, progressões aritméticas (PA) e progressões geométricas (PG), incluindo definições, classificações, termos gerais e somas. Esses conteúdos são fundamentais para o desenvolvimento de habilidades matemáticas sólidas e pensamento crítico.

A BNCC define que, durante toda a Educação Básica, devem ser desenvolvidas e aprimoradas 10 competências gerais. Essas competências abrangem áreas como conhecimento, pensamento científico, crítico e criativo, repertório cultural e habilidades de comunicação. Além disso, incluem a cultura digital e focam em aspectos como trabalho, projeto de vida, argumentação, autoconhecimento e autocuidado, empatia, responsabilidade e cidadania. A seguir temos a competência geral básica 1, a qual desdobra-se no tratamento didático proposto para as três etapas do ensino básico sobre a valorização e utilização dos conhecimentos históricos construídos sobre o mundo físico, social, cultural e digital.

> 1. Valorizar e utilizar os conhecimentos historicamente construídos sobre o mundo físico, social, cultural e digital para entender e explicar a realidade, continuar aprendendo e colaborar para a construção de uma sociedade justa, democrática e inclusiva. (BRASIL, 2017, p.9).

Notamos na competência geral básica 1, que cada conteúdo a ser apresentado surge a partir de um problema, seja teórico ou prático, historicamente construído. Compreender as questões que motivaram o estudo de um determinado conteúdo geralmente torna evidente sua aplicabilidade e, consequentemente, estimula os alunos a entendê-lo. Em nossas sugestões de abordagem, buscaremos apresentar problemas com valor prático e digital ao conteúdo em questão, adaptados ao nível de conhecimento dos estudantes do Ensino Médio.

De acordo com Brasil (2017), os alunos devem ser capazes de utilizar suas próprias formas de pensar, representar, comunicar e argumentar. Por meio de discussões e validações em grupo, espera-se que desenvolvam gradualmente conceitos, representações e procedimentos mais elaborados. No detalhamento das competências, afirma-se que, para desenvolver a habilidade de raciocinar, é essencial que os estudantes tenham a oportunidade de investigar, explicar e justificar as soluções encontradas para os problemas, em colaboração com colegas e professores, com foco nos processos de argumentação matemática.

A seguir temos a competência geral básica 5, que destaca a compreensão, utilização e criação de tecnologias digitais.

> 5. Compreender, utilizar e criar tecnologias digitais de informação e comunicação de forma crítica, significativa, reflexiva e ética nas diversas práticas sociais (incluindo as escolares) para se comunicar, acessar e disseminar informações, produzir conhecimentos, resolver problemas e exercer protagonismo e autoria na vida pessoal e coletiva. (BRASIL, 2017, p. 9).

A competência geral básica 5 da Base Nacional Comum Curricular (BNCC) enfatiza a importância de compreender, utilizar e criar tecnologias digitais de forma crítica, significativa, reflexiva e ética nas diversas práticas sociais. Essa competência abrange não apenas o acesso e a disseminação de informações, mas também a produção de conhecimentos, a resolução de problemas e o exercício de protagonismo tanto na vida pessoal quanto coletiva. Em um mundo cada vez mais digitalizado, os estudantes precisam ser capacitados a lidar com as tecnologias de informação e comunicação (TICs) de maneira que possam utilizar plataformas e ferramentas digitais para expressar ideias e interagir com outros, navegar com segurança em um vasto mar de informações, identificando fontes confiáveis e relevantes, criar conteúdo original e significativo, utilizando ferramentas digitais para pesquisa e apresentação, enfrentar desafios práticos, desenvolvendo soluções inovadoras com o apoio da tecnologia e exercer protagonismo e autoria agindo de forma ética no ambiente digital.

> Diante dessa realidade, o uso de tecnologias oferece caminhos para melhorar a qualidade da educação no Brasil. Elas não são uma solução ilimitada, mas podem impactar positivamente a eficiência educacional. Principalmente, elas abrem portas para a participação escolar de grupos sociais cujo acesso ao ensino regular foi historicamente negado. Segundo a UNESCO: "A forma como o sistema educacional incorpora as TIC afeta diretamente a redução da exclusão digital existente no país". Em resumo, a adoção de tecnologias digitais pode melhorar a qualidade da educação, e promover e impulsionar o desempenho escolar de todos os estudantes (CORREA; TANIGUTI; FERREIRA, 2021, p.25).

Assim, integrar a tecnologia do *Bitcoin* nas práticas pedagógicas pode enriquecer a experiência de aprendizagem, promovendo não apenas o domínio técnico, mas também a reflexão crítica e ética. Isso contribui para formar cidadãos mais conscientes e preparados para os desafios do mundo contemporâneo, alinhando-se aos objetivos da Competência Geral 5 da BNCC.

Competências específicas de Matemática e suas tecnologias no Ensino Médio descritos na BNCC:

> 1. Utilizar estratégias, conceitos e procedimentos matemáticos para interpretar situações em diversos contextos, sejam atividades cotidianas, sejam fatos das Ciências da Natureza e Humanas, das questões socioeconômicas ou tecnológicas, divulgados por diferentes meios, de modo a contribuir para uma formação geral.
>
> 2. Propor ou participar de ações para investigar desafios do mundo contemporâneo e tomar decisões éticas e socialmente responsáveis, com base na análise de problemas sociais, como os voltados a situações de saúde, sustentabilidade, das implicações da tecnologia no mundo do trabalho, entre outros, mobilizando e articulando conceitos, procedimentos e linguagens próprios da Matemática.
>
> 3. Utilizar estratégias, conceitos, definições e procedimentos matemáticos para interpretar, construir modelos e resolver problemas em diversos contextos, analisando a plausibilidade dos resultados e a adequação das soluções propostas, de modo a construir argumentação consistente.
>
> 4. Compreender e utilizar, com flexibilidade e precisão, diferentes registros de representação matemáticos (algébrico, geométrico, estatístico, computacional etc.), na busca de solução e comunicação de resultados de problemas.
>
> 5. Investigar e estabelecer conjecturas a respeito de diferentes conceitos e propriedades matemáticas, empregando estratégias e recursos, como observação de padrões, experimentações e diferentes tecnologias, identificando a necessidade, ou não, de uma demonstração cada vez mais formal na validação das referidas conjecturas. (BRASIL, 2017)

Segundo Lima (1999), o processo de ensino-aprendizagem da Matemática pode ser compreendido a partir de três eixos fundamentais: Conceituação, Manipulação e Aplicação. A construção conceitual está relacionada ao entendimento profundo dos significados matemáticos, enquanto a manipulação envolve a utilização técnica de algoritmos e procedimentos, e a aplicação diz respeito à capacidade de empregar tais conhecimentos em contextos reais e diversificados. Esses três pilares estão diretamente associados às competências gerais e específicas da Base Nacional Comum Curricular (BNCC), especialmente no que se refere à valorização da argumentação matemática, à resolução de problemas, à mobilização de diferentes registros de representação e ao desenvolvimento do pensamento crítico. Desse modo, ao incentivar os estudantes a investigar, explicar e justificar suas soluções, o professor promove uma prática pedagógica alinhada às três dimensões propostas por Lima (1999). Essa abordagem contribui para uma aprendizagem matemática mais significativa, contextualizada e voltada à formação integral do estudante.

2.1 Sequência e Progressões no Ensino da Matemática

A compreensão profunda de Sequências e Progressões é essencial na formação matemática básica e avançada. Essa temática, frequentemente abordada nos anos finais do Ensino Fundamental e, de maneira mais sistemática, no Ensino Médio, representa não apenas um conteúdo específico, mas também uma ponte para compreensão de funções, limites e, posteriormente, cálculo. Neste seção, exploramos o embasamento teórico que sustenta a escolha metodológica e pedagógica da abordagem das Sequências e Progressões em uma sequência didática contextualizada.

O estudo das Sequências e Progressões permite o desenvolvimento do pensamento algébrico e da capacidade de generalização dos estudantes. Pois,

> Ao contrário do conhecimento físico, a construção do conhecimento lógico necessita da abstração reflexiva. Isso quer dizer que, então, o sujeito já precisa ter capacidade para estabelecer relações entre dois objetos e para distinguir similaridades ou diferenças entre eles (BALESTRA, 2007, p. 26).

O processo de ensino-aprendizagem considera diversas variáveis que influenciam as interações e a organização do ambiente educacional.

> por exemplo: uma exposição, um debate, uma leitura, uma pesquisa bibliográfica, tomar notas, uma ação motivadora, uma observação, uma aplicação, um exercício, o estudo, etc. Desta maneira, podemos definir as atividades ou tarefas como uma unidade básica do processo de ensino/aprendizagem, cujas diversas variáveis apresentam estabilidade e diferenciação: determinadas relações interativas professor/alunos e alunos/alunos, uma organização grupal, determinados conteúdos de aprendizagem, certos recursos didáticos, uma distribuição do tempo e do espaço, um critério avaliador; tudo isto em torno de determinadas intenções educacionais, mais ou menos explícitas. (ZABALA, 1998, p. 22)

A BNCC apresenta, entre suas competências gerais, a necessidade de os estudantes desenvolverem o pensamento científico, crítico e criativo. Em Matemática, as habilidades previstas para o Ensino Médio incluem a identificação e compreensão de regularidades em diferentes contextos e a resolução de problemas com base em argumentos lógicos e matemáticos. A abordagem de sequências e progressões, portanto, está plenamente alinhada às diretrizes nacionais para a educação.

O conteúdo matemático deve partir de situações significativas e contextualizadas, respeitando o conhecimento prévio dos estudantes, podendo utilizar recursos tecnológicos e tecnologia educacional que facilitem o ensino-aprendizagem. Essa visão dialoga com Ramos,

> Entende-se por tecnologia educacional, o conjunto de técnicas, processos e métodos que utilizam meios digitais e demais recursos como ferramentas de apoio aplicadas ao ensino, com a possibilidade de atuar de forma metódica entre quem ensina e quem aprende. (RAMOS, 2012, p. 6)

Trabalhar com recursos tecnológicos em sala de aula não é uma tarefa tão simples, é necessário construir um planejamento estratégico de forma que os alunos e professores utilizem esses recursos como mediador do ensino-aprendizagem. Pois,

> Os alunos usam seus aparelhos para outras funções e pouco se presencia o professor propondo trabalhar com tais recursos tecnológicos. Porém, não é uma tarefa tão simples, pois necessita a construção de um projeto educacional coletivo que inclua a tecnologia como mediadora do ensino-aprendizagem. (RAMOS, 2012, p. 11)

Em nossa proposta didática, o uso de recursos tecnológicos (Celular e TVs) foi integrado como ferramenta de exploração e verificação de propriedades das sequências numéricas, em sintonia com as orientações da BNCC.

Do ponto de vista conceitual, sequências são funções cujo domínio é um conjunto dos números naturais e cujos elementos são definidos segundo uma determinada lei de formação. PA e PG são casos particulares de sequências, amplamente explorados devido à sua regularidade e aplicação em situações do cotidiano, como parcelamentos, crescimento populacional e previsões econômicas.

Reconhecemos a importância pedagógica de situar o conceito antes de apresentar sua definição formal, portanto buscamos uma maneira eficaz de introduzir a noção de sequências. Nessa dissertação seguimos a sugestão de apresentar sequências por meio de diferentes registros de representação semiótica com o uso de listas.

> Para isso, apresentaremos exemplos variados, os quais serão representados por meio de diferentes registros representação semiótica, incluindo ´ o uso de "listas", por se tratar de uma noção conhecida pelos alunos e que pressupõe posicionamento de cada elemento como parte da sua formação. (MARQUES, 2019, p. 45).

Podemos destacar que, ao trabalhar sequências e progressões, o professor pode favorecer a compreensão de estruturas matemáticas mais complexas, desde que a apresentação do conteúdo seja progressiva e fundamentada em exemplos diversos. Por exemplo, na modelagem de fenômenos tecnológicos, como o processo de *halving* do *Bitcoin*, que pode ser descrito por uma progressão geométrica de razão 1. Essa abordagem conduz naturalmente à discussão da soma de termos infinitos de uma PG, permitindo compreender a convergência para um valor máximo (no caso do *Bitcoin*, o limite de 21 milhões de unidades). Dessa forma, ao ampliar gradualmente o nível de abstração, a prática pedagógica possibilita que os estudantes transitem de situações simples para conceitos mais sofisticados, evitando uma compreensão restrita e promovendo uma visão integrada das estruturas matemáticas. Essa pluralidade de situações é essencial para evitar que os estudantes construam uma compreensão limitada dos conceitos.

A proposta da Paraíba (2021) também enfatiza a importância de respeitar o contexto local e promover uma aprendizagem significativa e contextualizada. Neste sentido, a sequência didática desenvolvida para o presente trabalho buscou vincular o estudo das sequências e progressões com situações reais, tecnológicas e próximas à realidade dos alunos da escola investigada.

> O que deveríamos buscar é oferecer a esses alunos atividades interessantes baseadas na Internet e, se quisermos alavancar o "aprender a aprender", precisamos levar em consideração que isso acontece de forma mais natural quando você e outro participante estão situados em uma mesma sintonia de ideias. (RODRIGUES, 2014, p.26)

E, vale destacar a contribuição da tecnologia no ensino de matemática: a utilização de ferramentas computacionais para análise de dados e representação gráfica pode tornar o processo de ensino-aprendizagem mais dinâmico e efetivo.

Assim, utilizamos a cadeia de blocos do *Bitcoin* como recurso digital e tecnológico em situações em que o conceito de sequências e progressões é crucial para o desenvolvimento da tecnologia tornando a aprendizagem lúdica e prática. A própria estrutura da cadeia de blocos do *Bitcoin* é formada por uma sequência ordenada de blocos, em que cada bloco contém um conjunto de transações e uma referência criptográfica ao bloco anterior, formando uma cadeia contínua. Essa estrutura sequencial é essencial para o funcionamento da rede, pois garante a integridade e a imutabilidade dos dados.

Ao estudar sequências e progressões, por exemplo, podemos associar cada bloco a um termo de uma sequência. O crescimento da cadeia de blocos pode ser comparado a uma progressão temporal, onde a adição de novos blocos ocorre a intervalos regulares de tempo (em média, a cada 10 minutos).

Dessa forma, a abstração matemática de sequências e progressões ganha um significado prático quando associada ao funcionamento da *Blockchain*, permitindo que o aluno compreenda esses conceitos por meio de uma aplicação concreta e atual da tecnologia.

2.2 Pesquisa bibliográfica sobre o termo bitcoin no banco de dados de dissertação do PROFMAT

No desenvolvimento do referencial teórico deste trabalho, realizamos uma pesquisa bibliográfica com o objetivo de identificar dissertações de mestrado que abordam o tema Bitcoin, buscando fundamentar a discussão com produções acadêmicas nacionais recentes e relevantes. Para isso, utilizamos o sistema de busca de dissertações do PROFMAT (Programa de Mestrado Profissional em Matemática em Rede Nacional), utilizando o termo *bitcoin* como palavra-chave.

A pesquisa resultou na identificação de dois trabalhos diretamente relacionados ao tema: a dissertação de Raoni do Nascimento Gonzaga, intitulada *Bitcoin*: uma introdução à matemática das transações, defendida na PUC em 2021, e a dissertação de Luiz Carlos da Silva Leao, intitulada Uma introdução ao estudo de bitcoins e blockchains, defendida na UNIRIO em 2019. Ambos os trabalhos estão disponíveis em formato PDF para consulta integral.

O trabalho de Gonzaga (2021) , intitulado *Bitcoin*: uma introdução à matemática das transações, apresenta uma análise detalhada dos fundamentos matemáticos que sustentam as transações de *Bitcoin*, com ênfase na aplicação da criptografia por curvas elípticas e do algoritmo ECDSA (Elliptic Curve Digital Signature Algorithm). A dissertação explora conceitos como grupos, corpos, problemas do logaritmo discreto e a geração de chaves públicas, demonstrando como esses elementos matemáticos garantem a segurança e a autenticidade das transações na rede Bitcoin. O estudo também contextualiza o funcionamento do blockchain e a emissão de bitcoins, fornecendo uma base teórica sólida para o entendimento da tecnologia subjacente às criptomoedas.

A dissertação de Leão (2019), intitulada Uma introdução ao estudo de bitcoins e blockchains, apresenta uma abordagem didática e abrangente sobre os fundamentos do Bitcoin e da tecnologia *Blockchain*. O trabalho se inicia explicando o funcionamento básico do blockchain e seus princípios fundamentais, seguido por uma revisão detalhada dos conceitos de criptografia, incluindo criptografia de chave pública, funções hash criptográficas (RIPEMD-160 e SHA-256) e assinaturas digitais. Além disso, o estudo aborda a estrutura das transações de Bitcoin, a formação dos blocos e o sistema de endereços, contextualizando esses elementos com exemplos práticos e sugerindo uma didática para o ensino da tecnologia em ambientes educacionais. A dissertação também discute a relevância da *blockchain* para a educação superior e propõe direções para estudos futuros, consolidando-se como uma importante referência para a compreensão técnica e pedagógica da criptomoeda e da tecnologia que a sustenta.

Na seleção dessas dissertações seguimos critérios de relevância temática e atualidade, considerando a pertinência dos trabalhos para o aprofundamento dos conceitos matemáticos e tecnológicos relacionados ao bitcoin e à tecnologia *Blockchain*. Conforme orientações metodológicas de pesquisa bibliográfica, a identificação, seleção e análise dessas fontes permitem mapear o estado atual do conhecimento científico sobre o tema, além de fornecer embasamento teórico para a discussão e análise desenvolvidas neste estudo. Assim, esta pesquisa bibliográfica realizada no banco de dados do PROFMAT contribui para situar o leitor quanto às produções acadêmica no contexto do programa nacional de mestrado profissional em matemática sobre *Bitcoin*, além de garantir o rigor científico e a fundamentação teórica necessária ao desenvolvimento do trabalho.

Diferentemente dos trabalhos de Gonzaga (2021) e Leão (2019), que abordam principalmente os fundamentos matemáticos da criptografia, das curvas elípticas, das funções hash e da estrutura técnica das transações e do *Blockchain*, este trabalho se distingue por integrar conceitos matemáticos clássicos do Ensino Médio, como sequências numéricas, progressões aritméticas e geométricas com a tecnologia *Blockchain* do *bitcoin*. Nessa dissertação propomos uma abordagem didática inovadora que utiliza a cadeia de blocos como ferramenta para o ensino prático e contextualizado da matemática, buscando desenvolver habilidades críticas e tecnológicas em estudantes do Ensino Médio por meio de aulas expositivas, atividades práticas e avaliações formativas. Enquanto os estudos anteriores focam na matemática avançada que sustenta a segurança e o funcionamento do Bitcoin, este trabalho enfatiza a aplicação pedagógica de conceitos matemáticos elementares, relacionando-os diretamente com o funcionamento da *mempool* e da *Blockchain*. Além disso, apresenta uma análise dos resultados obtidos com os alunos, avaliando a eficácia da metodologia proposta para o ensino da matemática contextualizada com tecnologias emergentes. Dessa forma, contribui para ampliar o leque de possibilidades didáticas no ensino da matemática, aproximando conteúdos tradicionais da realidade tecnológica atual.

3 Sequências e Progressões

Neste capítulo, iniciamos a formalização dos conceitos relacionados a sequências e progressões. Consideramos que, por meio das definições matemáticas rigorosas, é possível abordar a resolução de situações-problema de maneira mais eficaz, favorecendo a construção de argumentos lógicos e coerentes.

É importante destacar que tais definições constituem ferramentas fundamentais para a demonstração de propriedades relevantes, contribuindo significativamente para o desenvolvimento do pensamento crítico e do raciocínio lógico dos estudantes. As formulações, propriedades e resultados aqui apresentados estão fundamentados nas obras adotadas na disciplina de Matemática Discreta do PROFMAT (CARVALHO; MORGADO, 2017) , bem como na dissertação de mestrado de Camila Paulino Marques (MARQUES, 2019), que discute a relevância da Análise Real na formação do professor de Matemática do Ensino Médio, especialmente no contexto das sequências numéricas.

3.1 Sequência

Nesta seção, apresentaremos a definição de sequência, um conceito fundamental para diversos ramos da matemática, pois permite identificar padrões, descrever regularidades e generalizar comportamentos numéricos. Uma sequência pode ser entendida como uma lista ordenada de números, na qual cada elemento ocupa uma posição específica e, geralmente, segue uma regra de formação bem definida, conhecida como lei de recorrência ou lei de formação. Essas listas podem ser finitas ou infinitas, e apresentam diferentes comportamentos, como crescimento, decrescimento, constância ou oscilação. Apresentamos uma sequência de maneira informal, como listas, traremos a definição formal apresentada a seguir, para garantirmos o rigor matemático.

Definição 3.1. *Uma* ***sequência numérica*** *é uma função cujo domínio é o conjunto dos números naturais* $\mathbb{N}$*, no caso de sequências infinitas, ou o conjunto* $\{1, 2, \ldots, n\}$*, no caso de sequências finitas com* n *elementos. O contradomínio da função é o conjunto dos números reais* $\mathbb{R}$*.*

Notações Utilizadas

- $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$: denota o conjunto dos números naturais;
- $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$: denota o conjunto dos números inteiros;
- $\mathbb{Q}$: denota o conjunto dos números racionais;

- $\mathbb{R}$: denota o conjunto dos números reais;
- a_1: é o primeiro termo ou o termo de ordem 1;
- a_2: é o segundo termo ou o termo de ordem 2;
- a_n: é o n-ésimo termo da sequência, onde $n \in \mathbb{N}$.

Definição 3.2 Uma sequência $\{a_n\}$ é dita **monótona** quando se enquadra em uma das seguintes classificações:

- **Crescente**: se $a_n < a_{n+1}$, para todo $n \in \mathbb{N}$;
- **Não decrescente**: se $a_n \leq a_{n+1}$, para todo $n \in \mathbb{N}$;
- **Decrescente**: se $a_n > a_{n+1}$, para todo $n \in \mathbb{N}$;
- **Não crescente**:se $a_n \geq a_{n+1}$, para todo $n \in \mathbb{N}$.

Seguindo a sugestão de Marques (2019), optamos por nos referir inicialmente às sequências numéricas como "listas", com o intuito de utilizar uma terminologia mais acessível aos alunos do ensino médio. Tal abordagem busca facilitar a compreensão inicial do conceito formal de sequência, promovendo uma transição gradual do informal ao rigor matemático. A utilização do termo "lista" se mostra eficaz na introdução do conteúdo, especialmente quando aliada a exemplos contextualizados, conforme orienta a BNCC, nas competências que incentivam o uso da criatividade intelectual e a resolução de problemas por meio de situações reais. Essa estratégia didática visa tornar os conceitos mais naturais e significativos aos estudantes, preparando-os para a assimilação das definições formais posteriormente apresentadas.

A sequência de Fibonacci é uma sucessão numérica em que cada termo, a partir do terceiro, é obtido pela soma dos dois anteriores. Ela começa com 0 e 1, formando a sequência: 0, 1, 1, 2, 3, 5, 8, 13, 21... e assim por diante. Por exemplo, se temos os termos 5 e 8, o próximo será 5+8=13. Essa sequência aparece em diversos contextos da natureza, como na disposição das folhas em algumas plantas ou no formato das conchas, além de ter aplicações em matemática, computação e até mesmo em finanças.

Essa sequência foi utilizada como ponto de partida para a primeira aula da sequência didática, em razão de seu caráter acessível, histórico e interdisciplinar. Sua origem remonta ao matemático Leonardo de Pisa, conhecido como Fibonacci, que a apresentou no Liber Abaci (1202), obra traduzida para o inglês por Sigler (2002). A escolha dessa sequência visa despertar o interesse dos estudantes ao apresentar um conteúdo matemático por meio de uma situação-problema instigante e contextualizada, favorecendo a construção do conhecimento de forma significativa.

Além de promover a familiarização com conceitos como regularidade, padrões e recorrência, o estudo da sequência de Fibonacci possibilita a exploração de diferentes formas de representação e raciocínio matemático, conforme propõem as competências gerais da BNCC . Nesse sentido, a proposta didática contempla não apenas o desenvolvimento do conteúdo, mas também o estímulo à argumentação, à modelagem e à investigação, aspectos fundamentais para a formação crítica dos estudantes.

3.2 Progressões

A noção de progressão refere-se a uma sequência numérica que apresenta uma regularidade definida, estabelecida por meio de uma regra de formação. No contexto do ensino de Matemática, as progressões são classificadas de acordo com essa regularidade, sendo as mais conhecidas a progressão aritmética e a progressão geométrica.

A progressão aritmética é um conceito específico no estudo das sequências numéricas, amplamente utilizado para modelar fenômenos que apresentam crescimento ou decrescimento linear. Trata-se de uma sequência em que a diferença entre termos consecutivos é constante, valor esse denominado razão da progressão. Essa característica confere à PA uma estrutura regular e previsível, permitindo a formulação de expressões matemáticas para determinar qualquer termo da sequência, bem como a soma de seus termos. As progressões aritméticas podem ser finitas, quando possuem um número limitado de termos, ou infinitas, quando se estendem indefinidamente. A compreensão desse tipo de sequência é essencial para diversas áreas da matemática e suas aplicações práticas, servindo como base para o desenvolvimento de conceitos mais avançados. Na seção a seguir, será apresentada a definição formal da progressão aritmética, acompanhada e principais propriedades.

Definição 3.2. ***Progressão Aritmética*** *é uma sequência onde a diferença entre cada termo e o termo anterior é constante. Essa diferença constante é chamada de razão da progressão e é representada pela letra r.*

Em uma progressão aritmética $(a_1, a_2, a_3, \dots)$, cada termo, a partir do segundo, é obtido somando-se ao anterior uma constante denominada **razão da progressão**, representada por r. O termo geral de uma progressão aritmética é dado por:

$$a_n = a_1 + (n-1)r,$$

onde:

- a_n é o n-ésimo termo da progressão;
- a_1 é o primeiro termo;

- r é a razão comum;
- n é a posição do termo na sequência.

A mesma fórmula pode ser aplicada para calcular termos anteriores ou posteriores a qualquer termo conhecido da progressão.

A seguir faremos a demonstração da fórmula do termo geral da PA. Considere uma progressão aritmética com primeiro termo a_1 e razão r. Os termos dessa sequência são obtidos somando sucessivamente a razão ao termo anterior. Assim, temos:

$$\begin{aligned}
a_1 &= a_1, \\
a_2 &= a_1 + r, \\
a_3 &= a_2 + r = a_1 + 2r, \\
a_4 &= a_3 + r = a_1 + 3r, \\
&\vdots \\
a_n &= a_1 + (n-1)r.
\end{aligned}$$

A partir desse padrão, observa-se que o n-ésimo termo da progressão é dado por:

$$a_n = a_1 + (n-1)r.$$

Portanto, a fórmula do termo geral da PA está conjecturada por meio da construção dos termos da sequência.

Demonstração. Considere a propriedade $P(n)$: $a_n = a_1 + (n-1)r$, vamos provar, por indução, que $P(n)$ é verdadeira para todo $n \geq 1$.

Base: Para $n = 1$ temos $a_1 = a_1 + (1-1)r = a_1 + 0 = a_1$, logo $P(1)$ vale.

Passo indutivo: Suponha que $P(k)$ seja verdadeira para algum $k \geq 1$, ou seja, $a_k = a_1 + (k-1)r$. Então, usando a relação da progressão aritmética,

$$a_{k+1} = a_k + r = \big(a_1 + (k-1)r\big) + r = a_1 + kr = a_1 + ((k+1)-1)r.$$

Portanto $P(k+1)$ vale. Pelo princípio da indução, $P(n)$ vale para todo $n \geq 1$, ou seja, $a_n = a_1 + (n-1)r$ para todo n natural.

■

Baseando-nos na ideia de Gauss, usada para calcular a soma $1 + 2 + \cdots + 100$, podemos generalizar para determinar a soma dos n primeiros termos de uma progressão aritmética qualquer.

Teorema 3.1. *A soma dos n primeiros termos da progressão aritmética $(a_1, a_2, a_3, \ldots)$ é dada por:*

$$S_n = \frac{(a_1 + a_n)n}{2}.$$

Demonstração. Seja a soma dos n primeiros termos:

$$S_n = a_1 + a_2 + a_3 + \cdots + a_{n-1} + a_n.$$

Escrevendo a mesma soma de trás para frente:

$$S_n = a_n + a_{n-1} + a_{n-2} + \cdots + a_2 + a_1.$$

Somando membro a membro essas duas expressões, temos:

$$2S_n = (a_1 + a_n) + (a_2 + a_{n-1}) + (a_3 + a_{n-2}) + \cdots + (a_{n-1} + a_2) + (a_n + a_1).$$

É possível notar que as somas de termos começando por $a_1 + a_n$ até $a_n + a_1$, todas coincidem, isto é, cada par resulta na mesma soma, pois estamos agrupando o primeiro termo com o último, o segundo com o penúltimo, o terceiro com o antepenúltimo, e assim por diante.

Essa simetria acontece porque estamos lidando com uma **progressão aritmética**, onde a diferença entre os termos é constante. Assim, os termos equidistantes dos extremos têm a mesma média, o que garante que suas somas sejam sempre iguais. Como há n termos no total, formamos n pares iguais a a_1+a_n ao fazer essa reordenação da soma da sequência duas vezes.

Portanto, como há n desses pares, segue que:

$$2S_n = (a_1 + a_n) \cdot n \quad \Rightarrow \quad S_n = \frac{(a_1 + a_n)n}{2}.$$

■

A progressão geométrica é um tipo de sequência numérica em que cada termo, a partir do segundo, é obtido pela multiplicação do termo anterior por uma constante chamada razão. Essa característica faz com que os termos cresçam ou decresçam de forma multiplicativa, diferentemente da progressão aritmética, em que a variação é aditiva. As progressões geométricas podem ser finitas ou infinitas, e possuem fórmulas específicas para o cálculo do termo geral e da soma dos termos. O estudo das PGs é essencial para diversas áreas da matemática e suas aplicações, como finanças, física e ciências da computação. A seguir apresentamos sua definição formal.

Definição 3.3. *Uma* ***Progressão Geométrica*** *é uma sequência numérica da forma*

$$(a_1, a_2, a_3, \ldots),$$

em que, a partir do segundo termo, cada termo é obtido pela multiplicação do termo anterior por uma constante q, chamada de razão da PG. Isto é, para todo $n \geq 2$, vale:

$$a_n = a_{n-1} \cdot q.$$

Definição 3.4. *O termo geral de uma progressão geométrica* $(a_1, a_2, a_3, \ldots)$ *é dado por:*

$$a_n = a_1 \cdot q^{n-1},$$

onde a_1 *é o primeiro termo da PG,* q *é a razão, e* $n \in \mathbb{N}^*$*.*

A soma dos termos de uma progressão geométrica finita é um conceito fundamental para o estudo das sequências multiplicativas, permitindo calcular o total acumulado de uma série de valores que seguem uma razão constante. Considerando uma PG com um número finito de termos, essa soma pode ser expressa por uma fórmula fechada que facilita o cálculo sem a necessidade de somar termo a termo. Essa propriedade é amplamente utilizada em diversas áreas, como finanças, para o cálculo de juros compostos, e em problemas de física e engenharia que envolvem processos exponenciais. Em seguida, apresentaremos a fórmula geral para a soma dos termos de uma PG finita.

Teorema 3.2. *Seja* $(a_1, a_2, a_3, ...a_n)$ *uma progressão geométrica de* n *termos com razão* $q \neq 1$*. A soma dos* n *primeiros termos é dada por:*

$$S_n = \frac{a_1(1-q^n)}{1-q}.$$

Demonstração. Considere a soma:

$$S_n = a_1 + a_1q + a_1q^2 + \cdots + a_1q^{n-1}.$$

Multiplicando ambos os lados por q, temos:

$$qS_n = a_1q + a_1q^2 + a_1q^3 + \cdots + a_1q^n.$$

Subtraindo as duas igualdades:

$$S_n - qS_n = a_1 - a_1q^n \to \ S_n(1-q) = a_1(1-q^n).$$

Como $q \neq 1$, temos:

$$S_n = \frac{a_1(1-q^n)}{1-q}.$$

■

O estudo da soma dos termos de uma PG tem duas conclusões: se a razão tem módulo maior do que ou igual 1, então a soma diverge, isto é, não se aproxima de nenhum valor real; por outro lado, se a razão tem módulo menor do que 1 Nesses casos, é possível determinar um valor finito para a soma de infinitos termos, o que tem aplicações importantes em áreas como cálculo, séries infinitas, economia e ciências aplicadas. O estudo dessa soma pode auxiliar na compreensão de comportamentos assintóticos e limites de processos que se aproximam de um valor constante. Em seguida apresentaremos a fórmula que permite calcular esse somatório.

Teorema 3.3. *Se a progressão geométrica for infinita e a razão q satisfizer $|q| < 1$, então a soma da PG infinita é dada por:*

$$S = \frac{a_1}{1-q}.$$

Demonstração. Neste caso, tomamos o limite da soma finita quando $n \to \infty$:

$$S = \lim_{n\to\infty} \frac{a_1(1-q^n)}{1-q}.$$

Como $|q| < 1$, então $q^n \to 0$ quando $n \to \infty$, logo:

$$S = \frac{a_1(1-0)}{1-q} = \frac{a_1}{1-q}.$$

∎

4 A Rede do Bitcoin

Neste capítulo, abordaremos a **rede do *Bitcoin*** entendendo-a como uma cadeia de blocos interligados e o termo *bitcoin* como uma moeda digital que pode ser enviada de pessoa para pessoa. Detalharemos seus fundamentos, um pouco da sua história, seu funcionamento e os aspectos matemáticos associados. Inicialmente, apresentamos os conceitos básicos da rede idealizada por Satoshi Nakamoto, que permite pagamentos eletrônicos diretos entre pessoas sem intermediários utilizando essa rede. Discutiremos aspectos econômicos do *bitcoin* como dinheiro digital e a identidade misteriosa de seu criador. Em seguida, explicaremos o procedimento completo de uma transação e a segurança proporcionada pela criptografia e transparência da rede.

Por fim, apresentamos uma conexão entre **rede do *Bitcoin*** e conceitos matemáticos de sequências e progressões, interpretando os blocos como termos de uma sequência ordenada e encadeada no tempo. Isso permite analisar a estrutura da rede sob uma perspectiva matemática, compreendendo seu crescimento acumulado e a dependência entre blocos consecutivos. Essa abordagem oferece uma visão integrada dos fundamentos técnicos do *Bitcoin* e sua relação com conceitos matemáticos de sequências e progressões.

Nos Quadros 1 e 2 apresentamos os principais termos técnicos abordados neste documento, com o objetivo de facilitar a compreensão do leitor.

Quadro 1 – Principais termos técnicos

Termos técnicos da rede Bitcoin	
Termo Técnico	**Descrição**
Criptografia	Técnica matemática que protege as transações, garantindo segurança e privacidade.
Chave privada	Código secreto que permite movimentar os bitcoins de uma carteira.
Chave pública	Código visível a todos, usado para receber bitcoins.
Assinatura digital	Prova criptográfica que autentica uma transação, garantindo que foi feita pelo dono da chave privada.
Proof of Work (Prova de Trabalho)	Mecanismo que exige esforço computacional dos mineradores para validar blocos.

Fonte: Elaborado pelo próprio autor.

Quadro 2 – Principais termos técnicos sobre

Termos técnicos da rede Bitcoin	
Hash	Código alfanumérico gerado por uma função matemática, usado para identificar blocos e transações.
Blockchain	Registro público e imutável de todas as transações realizadas na rede Bitcoin.
Bloco gênese	Primeiro bloco da rede Bitcoin, minerado por Satoshi Nakamoto em 2009.
Bloco	Conjunto de transações agrupadas e registradas na blockchain.
Node (Nó)	Computador que participa da rede Bitcoin, ajudando a validar e propagar transações e blocos.
Mempool	Área temporária da rede onde ficam as transações que aguardam confirmação.
Minerador	Participante que usa poder computacional para validar blocos e receber recompensas.
Pool de mineração	Grupo de mineradores que unem seus recursos para aumentar as chances de minerar blocos.
Halving	Evento que reduz pela metade a recompensa por bloco a cada 210.000 blocos minerados.
Recompensa por bloco	Quantidade de bitcoins recebida pelo minerador que valida um bloco.
Taxas de transação	Valor pago pelos usuários para priorizar a inclusão de suas transações em um bloco.
Seed phrase (Frase-semente)	Conjunto de 12 palavras que permite restaurar uma carteira de bitcoin.
BIP-39	Padrão que define como as frases mnemônicas (seed phrases) são geradas a partir da chave privada.
BIP-32	Padrão que permite criar carteiras com múltiplos endereços derivados de uma chave principal.
Bech32	Formato moderno de endereço Bitcoin, iniciando com `bc1`, mais eficiente e seguro.
Confirmações de transação	Número de blocos adicionados à blockchain após o bloco que contém uma transação.
Gasto Duplo	Tentativa de enviar uma cópia de bitcoin
Dificuldade da rede	Medida que ajusta a complexidade da mineração para manter o tempo médio de 10 minutos por bloco.
Transação	Transferência de bitcoin de um endereço de carteira para outro.
Carteira de bitcoin	softwares que podem criar endereços públicos e privados de bitcoin, visualizar e movimentar saldos.

Fonte: Elaborado pelo próprio autor.

4.1 Fundamentos e história

A **rede do *Bitcoin*** foi idealizada por uma pessoa ou grupo sob o pseudônimo Satoshi Nakamoto, com o propósito de permitir pagamentos eletrônicos diretos entre pessoas sem a necessidade de uma instituição financeira intermediária. Em 2008, Satoshi publicou o artigo *Bitcoin: A Peer-to-Peer Electronic Cash System*, descrevendo o funcionamento do sistema. Em 2009, o primeiro *software* de Bitcoin foi lançado e a primeira transação foi realizada. A identidade de Satoshi permanece desconhecida, e sua escolha por usar um pseudônimo adiciona um ar de mistério à criação do *Bitcoin.*

Satoshi definiu uma moeda eletrônica como: Uma cadeia de assinaturas digitais. (NAKAMOTO, 2008). Para fazer uma transação de *bitcoin* é necessário uma assinatura digital confirmadas nos blocos, a qual abordaremos adiante. O artigo original, *Bitcoin: A Peer-to-Peer Electronic Cash System* (NAKAMOTO, 2008), apresenta os principais componentes da rede: prova de trabalho (*Proof-of-Work*), *blockchain* (cadeia de blocos da rede *Bitcoin*) e validação (confirmação) descentralizada de transações.

Ulrich (2014), em *Bitcoin: A Moeda na Era Digital*, aprofunda os aspectos econômicos e tecnológicos do *bitcoin.* Ele destaca que a arquitetura descentralizada do *bitcoin* confere à moeda digital propriedades semelhantes às do ouro: escassez, divisibilidade, portabilidade e durabilidade, mas com a vantagem da digitalização e da transmissão instantânea global. Além disso, o autor aponta que a rede é baseada em incentivos econômicos. Os mineradores (agentes na rede que se utilizam de energia computacional para encaixar transação no bloco) competem para validar blocos de transações e recebem recompensas em *bitcoin*, o que garante segurança e integridade à rede.

O funcionamento do *bitcoin* pode ser explicado a partir de sua estrutura que opera em uma rede chamada *blockchain*, a qual é um banco de dados público e compartilhado onde todas as transações são registradas de forma segura e transparente. Cada bloco agrupa várias transações validadas e é adicionado à cadeia aproximadamente a cada 10 minutos. Essa cadeia é pública, imutável e protegida por criptografia, garantindo que as informações não possam ser alteradas retroativamente, essa rede pode ser observada na Figura 1. A Figura 1 é uma captura de tela da *blockchain* onde é possível observar blocos à direita da linha vertical tracejada que foram confirmadas na rede e à esquerda blocos que aguardam confirmação.

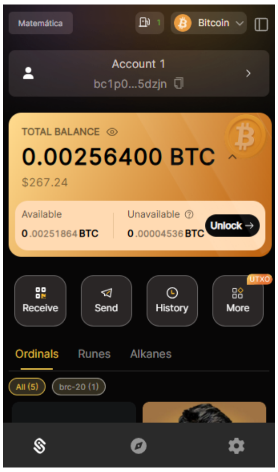
Figura 1 – Blockchain

Fonte: Elaborado pelo autor (2025)

As transações são feitas por meio de carteiras digitais que são *softwares* que podem ser instalados em computadores ou celulares. Cada carteira possui chaves privadas que garantem a propriedade e permitem assinar transações, provando que quem está gastando os *bitcoins* é o legítimo dono.

A Figura 2 mostra uma interface de carteira de *bitcoin*, onde são apresentadas informações sobre o saldo e as funcionalidades do aplicativo. No topo, é exibido o saldo total de 0.00256400 BTC, equivalente a $267.24, que representa o valor atual do *bitcoin* em dólares. Abaixo é possível observar quatro botões, *Receive* para receber *bitcoin*, *Send* para enviar *bitcoin*, *History* para ver o histórico da carteira e *More* para mais funcionalidades.

Figura 2 – carteira de *bitcoin*



Fonte: Elaborado pelo autor (2025)

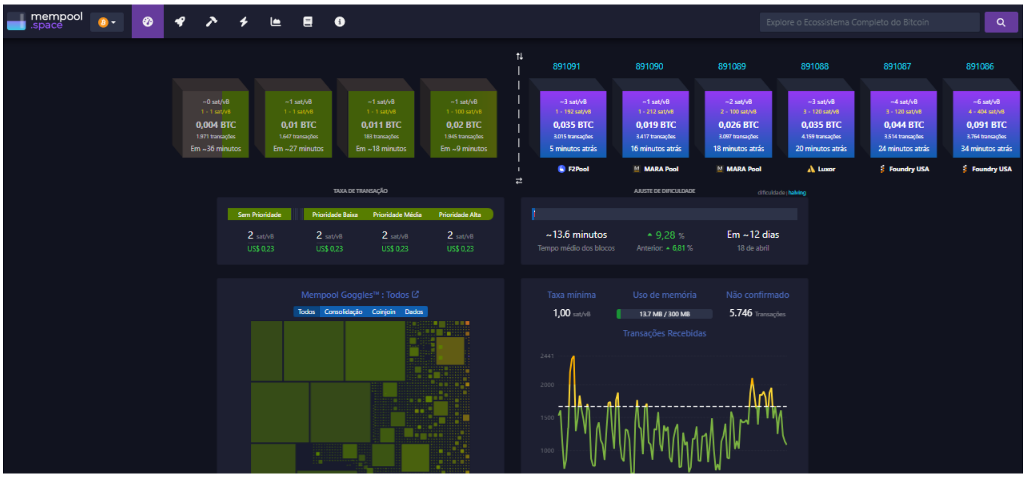
Uma transação é a transferência de *bitcoins* entre carteiras. Ela é assinada digitalmente com a chave privada do remetente para garantir segurança e autenticidade. Essas transações são divulgadas para a rede e precisam ser validadas para serem consideradas válidas.

4.2 A *Mempool* do *Bitcoin*

A *Mempool* (Memory Pool) é o espaço onde as transações ficam armazenadas temporariamente, aguardando serem incluídas em um bloco. Cada nó da rede mantém sua própria versão da *mempool*, e os mineradores priorizam as transações com maiores taxas (*fee rate*).

Para acompanhar o estado atual da *mempool*, podemos utilizar o explorador de blocos <https://mempool.space/pt>, que exibe visualmente o volume de transações pendentes e as taxas recomendadas para inclusão rápida. Podemos observar na Figura 3, blocos já confirmados à direita da linha vertical traceja e blocos à esquerda esperando confirmação, quadrados verdes, os quais representam transações de *bitcoin* sendo encaixadas no próximo bloco aguardando confirmação. Podemos observar a quantidade de taxas somadas das transações em cada bloco e a quantidade de transações que serão encaixadas nesse bloco.

Figura 3 – Visualização da *mempool*



Fonte: Elaborado pelo autor (2025)

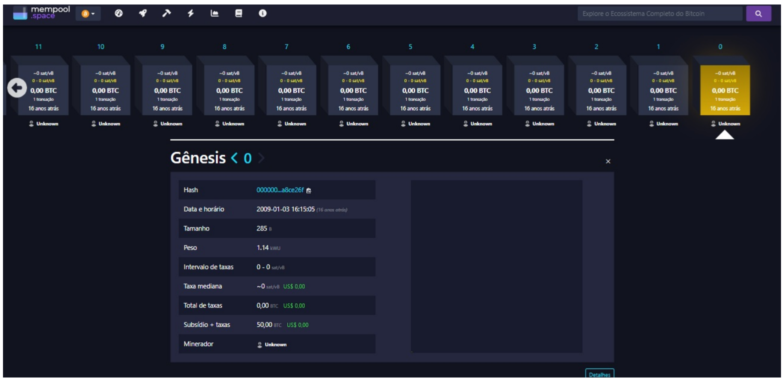
A *mempool* é fundamental para entender o funcionamento das taxas de rede. Quando a demanda por espaço em bloco aumenta, as taxas também aumentam, tornando a *mempool* uma espécie de fila dinâmica de transações.

4.2.1 O bloco gêneses

O primeiro bloco da rede *Bitcoin*, conhecido como *Bloco Gêneses* (*Genesis Block*), foi minerado por Satoshi Nakamoto em 3 de janeiro de 2009. Esse bloco contém a mensagem oculta: *The Times 03/Jan/2009 Chancellor on brink of second bailout for banks.* Essa mensagem refere-se à manchete do jornal britânico *The Times* do mesmo dia e é interpretada como uma crítica ao sistema financeiro tradicional.

Na Figura 4 é possível ver por meio da *mempool* o primeiro bloco da rede *Bitcoin*. Observamos o primeiro bloco na cor dourada minerado pelo Satoshi Nakamoto contendo apenas 1 transação. Ao clicarmos no bloco dourado é possível ver informações como data e horário da mineração (03/01/2009). Esse bloco é especial e não tem nenhum bloco anterior. Ele representa o nascimento da rede e marca o início de uma nova era para o dinheiro digital.

Figura 4 – Bloco gêneses do *Bitcoin*



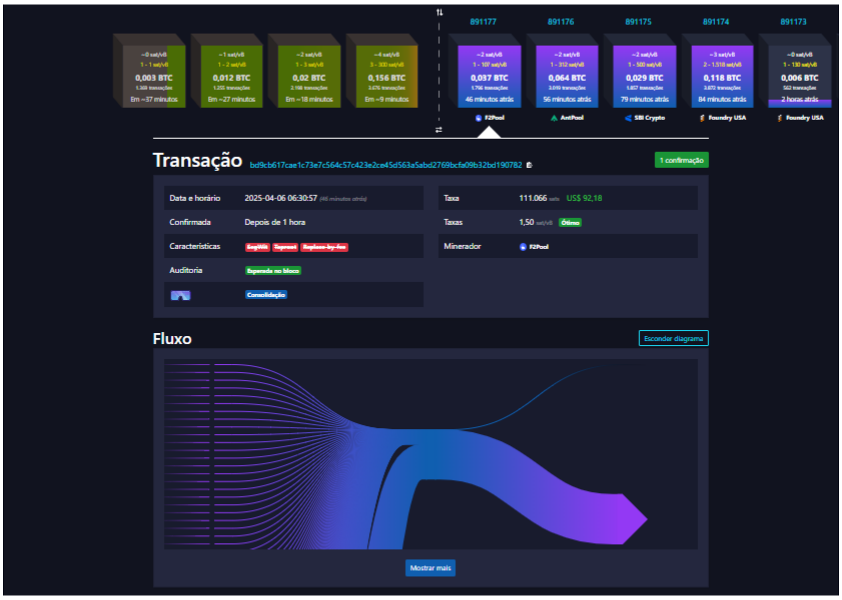
Fonte: Elaborado pelo autor (2024)

4.2.2 Transações em espera na rede *Bitcoin*

A rede *Bitcoin* funciona como uma grande **sala de jogos** onde todos os jogadores (os usuários de *Bitcoin*) se comunicam entre si. Quando alguém envia *bitcoin* para outra pessoa, essa informação precisa ser **registrada**, para que todos saibam que a transação aconteceu.

Na Figura 5 observarmos um bloco confirmado a direita da linha tracejada vertical, ao clicarmos nesse bloco, podemos observar 1796 transações que foram confirmadas com o bloco, data e horário que esse bloco foi confirmado, as taxas que o minerador F2Pool recebeu e o Fluxo das transações contidas no bloco.

Figura 5 – Um bloco confirmado na rede



Fonte: Elaborado pelo autor (2024)

4.3 Mineração

Para adicionar um bloco à *blockchain*, os mineradores precisam resolver um problema matemático, geralmente baseado em algoritmo. O objetivo é encontrar um *hash* que atenda a certos critérios, como começar com um número específico de zeros. Vários mineradores competem simultaneamente para resolver esse quebra-cabeça e o primeiro a encontrar uma solução válida recebe uma recompensa, que pode incluir novas moedas e taxas de transação. Uma vez que um minerador resolve o problema, o bloco é transmitido para a rede, onde outros nós verificam a validade das transações contidas nele e a solução do quebra-cabeça. Se a solução for verificada, o novo bloco é adicionado à *blockchain*, e o processo recomeça com um novo conjunto de transações. Esse processo garante a segurança e integridade da rede.

Na Figura 6, observamos, ao clicarmos no primeiro bloco aguardando confirmação, quadrados verdes de vários tamanhos, esses quadrados representam uma transação e o tamanho do quadrado representa o tamanho da taxa a ser paga para que essa transação seja confirmado dentro bloco, caso contrário a transação será encaminhada para o próximo bloco.

Figura 6 – Problema do encaixe das transações no bloco

Fonte: Elaborado pelo autor (2024)

A posição dos quadrados muda a cada segundo, isso representa o problema de encaixe e gasto de energia para encaixar de forma mais eficiente essas transações. Esse problema dura cerca de 10 (dez) minutos e caso o minerador resolva o problema antes dos 10 minutos ele pode aguardar completar os 10 minutos para confirmar a validação do bloco.

4.3.1 *Pools* de mineração

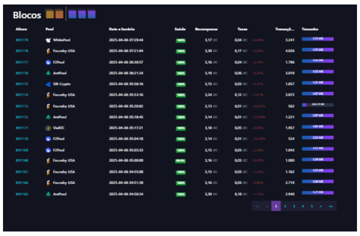
Pools de mineração de *bitcoin* são grupos de mineradores que se unem para aumentar suas chances de resolver o quebra-cabeça matemático necessário para adicionar um novo bloco à *blockchain*. Ao trabalhar juntos, eles combinam seu poder computacional, o que torna a resolução do problema mais rápida e eficiente. Quando a *Pools* consegue minerar um bloco, a recompensa é distribuída entre os membros de acordo com a contribuição de cada um.

Esse sistema é vantajoso, pois a mineração individual pode ser extremamente difícil e, muitas vezes, pouco lucrativa devido à alta concorrência. Com as *Pools*, os mineradores podem obter recompensas mais regulares, já que a probabilidade de encontrar um bloco é maior. Além disso, *Pools* de mineração geralmente têm taxas associadas, que são uma porcentagem da recompensa, mas isso é compensado pela maior frequência de pagamentos.

As *Pools* podem variar em tamanho e estrutura, e alguns têm regras específicas sobre como as recompensas são distribuídas, como sistemas de pagamento proporcional. Essa colaboração não só melhora a eficiência da mineração, mas também promove a descentralização da rede, já que mais pessoas têm a oportunidade de participar e receber recompensas.

Na Figura 7 observamos algumas *Pools* de mineração de *bitcoin*, na segunda coluna *Pool* encontramos o nome da *Pool* de mineração de *bitcoin*, como por exemplo, a *Pool* Antipool. Vale destacarmos que cada *Pool* contêm alguns mineradores que caso queiram sair podem sair a qualquer momento. Observamos outras informações como a saúde da *Pool* e taxas recebidas.

Figura 7 – *Pools* de mineração de *bitcoin*



Fonte: Elaborado pelo autor (2024)

4.3.2 Unidades de *bitcoin* (BTC) e recompensas

Após a confirmação do bloco, o minerador recebe taxas + subsídio (Taxa de uma transação de *bitcoin* por transações e uma recompensa com novos *bitcoin* surgindo na rede). O Satoshi Nakamoto ao escrever o código da rede *bitcoin* fixou que cada bloco será confirmado em aproximadamente 10 minutos e que a cada 210 mil blocos, o subsídio por bloco será reduzido pela metade (*halving*), iniciando o subsídio de 50 *bitcoin* (BTC) no bloco gênesis.

A seguir temos o cálculo do tempo total entre *halvings*:

$$210.000 \times 10 \text{ minutos} = 2.100.000 \text{ minutos.}$$

Convertendo para anos:

$$\begin{aligned} 2.100.000 \text{ minutos} &= \frac{2.100.000}{60} \text{ horas.} = 35.000 \text{ horas} \\ 35.000 \text{ horas} &= \frac{35.000}{24} \text{ dias} \approx 1458,33 \text{ dias.} \\ 1458,33 \text{ dias} &= \frac{1458,33}{365} \text{ anos} \approx 4 \text{ anos.} \end{aligned}$$

Assim, concluímos que um ciclo completo de *halving* leva cerca de 4 anos.

Na Figura 8, observamos que a Pool de mineração MARA recebeu 0,018 BTC de taxas de transação mais 3,125 BTC que surgiram na rede totalizando 3,143 BTC. Essa recompensa será distribuída para todos os mineradores que tem registro nessa Pool (MARA).

Figura 8 – Bloco confirmado pela MARA

Fonte: Elaborado pelo autor (2024)

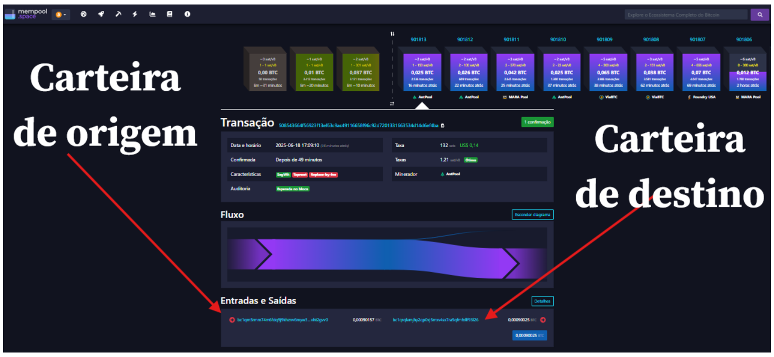
4.4 Por que o Bitcoin é seguro?

Em grego, *cryptos* significa secreto, oculto. A criptografia estuda os métodos para codificar uma mensagem de modo que só seu destinatário legítimo consiga interpretá-la. É a arte dos "códigos secretos" (COUTINHO, 2015). As transações do *bitcoin* são protegidas por técnicas de criptografia avançadas. Cada transação é assinada digitalmente com chaves criptográficas, garantindo que apenas o proprietário da moeda possa autorizar sua transferência. Todas as transações são públicas na *blockchain*. Porém, as identidades dos usuários não são reveladas. Ao clicarmos em um dos quadrados verdes dentro dos blocos podemos observar a transação de *bitcoin* de um endereço de carteira de origem para outro endereço de carteira de destino, ilustados na imagem a seguir retiradas da *mempool*.

Na Figura 9, observamos data, hora, quantidade de 0,00090157 BTC transferidos de um endereço para outro e a taxa paga pela transação, mas sem revelar as identidades dos endereços. Ao lado da palavra Transação há um resumo codificado do conjunto de informações contidas nessa transferência, o qual chamamos de *hash*.

> O Bitcoin, por outro lado, era absolutamente não reproduzível e construído de tal modo que seu registro histórico de transações possibilitava que cada unidade monetária fosse conciliada e verificada no decorrer da evolução da moeda. Ademais, e o que era essencial, a moeda residia em uma rede de código-fonte aberto, não sendo propriedade de ninguém em particular, removendo, assim, o problema de um ponto único de falha (ULRICH, 2014, p.14).

Figura 9 – Transferência de BTC de um acarteira para outra



Fonte: Elaborado pelo autor (2024)

4.4.1 Carteiras de bitcoin

Tradicionalmente, uma chave privada é uma sequência aleatória de 256 bits representada em hexadecimal (Sistema de numeração de base 16 que utiliza 16 símbolos, dos quais os números de 0 a 9 e as letras de a a f) , o que a torna difícil de memorizar e propensa a erros de transcrição por usuários não técnicos.

Para tornar esse processo mais acessível, foi desenvolvido o padrão BIP-39 (*Bitcoin Improvement Proposal 39*), que propõe uma forma mnemônica de representar chaves privadas. Esse padrão converte a entropia criptográfica (medida do grau de aleatoriedade ou imprevisibilidade de uma informação usada em criptografia), geralmente 128, 160, 192, 224 ou 256 bits em uma sequência de palavras escolhidas de um vocabulário padronizado contendo 2048 termos. A forma mais comum de representação mnemônica utiliza 128 bits de entropia, resultando em uma sequência de 12 palavras, conhecidas como *seed phrase* ou *mnemonic phrase*.

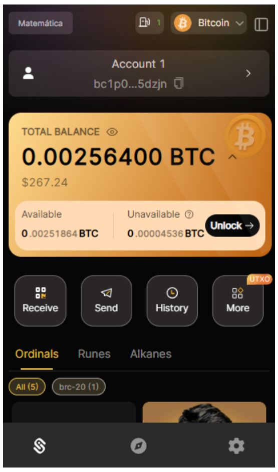
Essa frase de 12 palavras permite que o usuário recupere toda a carteira e suas chaves derivadas, com base em algoritmos determinísticos de geração de carteiras hierárquicas (padrão BIP-32). Assim, a frase mnemônica funciona como uma representação compacta e legível da chave privada mestra, a partir da qual todas as demais chaves da carteira podem ser derivadas de forma segura e padronizada.

Além de sua função prática, a adoção do padrão BIP-39 amplia significativamente a usabilidade e a segurança operacional no uso de carteiras, ao reduzir a complexidade técnica e permitir a realização de cópias de segurança confiáveis por parte do usuário. De forma resumida, uma carteira contém uma **chave privada** (secreta) e uma **chave pública** (visível para todos). A chave privada é representada por uma **frase mnemônica** com 12 palavras (padrão BIP-39).

Em seguida temos um exemplo de carteira privada de *bitcoin* escrita com letras e números: KzdaeX5nSc3k9RHVfd3ayp1iB8AsZq3yd3eyo1XYhkFuS6ZRXcY1: após a implementação de melhoria (BIP39), essa carteira pode ser associada a 12 palavras, galaxy banana twist echo rubber castle planet creek monkey velvet lion path. As quais podem ser decodificadas por uma carteira de *bitcoin*. Como um exemplo de endereço públicos derivada da chave privada, temos: bc1p0w9auldw6cm3hyu89s6h37xxcrflze42cdcjh5qz 6su2ss0jazqqx5dzjn , o qual é utilizado para receber *bitcoin*.

Um exemplo de carteira de código aberto é o **Unisat**, que permite gerenciar seus *bitcoin* com segurança. Ela pode ser baixada facilmente por lojas de aplicativos como playstore ou appstore. Na Figura 10 podemos observar o ambiente gráfico da carteira de bitcoin unisat.

Figura 10 – Carteira de bitcoin unisat



Fonte: Elaborado pelo autor (2024)

4.5 Procedimento de uma transação de bitcoin

Para iniciarmos uma transação de *bitcoin*, o usuário que deseja enviar *bitcoins*, abre sua carteira digital (*software*) e insere dois dados principais: a quantidade de *bitcoins* a ser enviada e o endereço público do destinatário (uma sequência alfanumérica que funciona como um identificador na rede). Ao clicar em enviar, a carteira utiliza a chave privada do remetente para assinar digitalmente a transação. Essa assinatura é uma prova criptográfica de que o remetente é o legítimo dono dos fundos e autoriza a transferência.

Após a assinatura, a transação é transmitida para um nó (node) da rede *Bitcoin* ao qual a carteira está conectada. Esse nó realiza uma validação inicial para checar se a transação está correta, ou seja, se o remetente possui saldo suficiente e se a assinatura é válida. Se aprovada, a transação é propagada para outros nós da rede, alcançando quase todos os participantes, garantindo sua divulgação ampla.

Após assinada as transações validadas ficam armazenadas na *mempool*, uma sala de espera onde aguardam para serem incluídas em um bloco pelos mineradores. A *mempool* funciona como um armazenamento temporário, e as transações com taxas (valor pago em *Bitcoin* pelo espaço no bloco) mais altas geralmente têm prioridade para serem selecionadas pelos mineradores, pois estes recebem essas taxas como recompensa.

Esses mineradores competem para resolver um problema matemático complexo (prova de trabalho) que permite validar (organizar as transações) um novo bloco contendo várias transações da *mempool*, incluindo a do remetente. O minerador que encontrar a solução primeiro anuncia o bloco para a rede. Essa etapa demora em média 10 minutos por bloco, dependendo da dificuldade da rede naquele momento. Após o problema de encaixe das transações no bloco resolvida pelo minerador, outros nós da rede verificam se o bloco e as transações contidas nele são válidos. Se aprovado, o bloco é adicionado à *blockchain*, que é o registro público e imutável de todas as transações. A transação do usuário recebe sua primeira confirmação nesse momento.

Cada bloco novo adicionado após o bloco que contém a transação representa uma confirmação adicional, aumentando a segurança contra tentativas de reversão ou fraude. A prática comum é esperar seis confirmações (aproximadamente uma hora) para considerar a transação irreversível, pois a probabilidade de alteração após esse ponto é praticamente nula devido ao alto custo computacional necessário. Após as confirmações, o destinatário pode visualizar e utilizar os *bitcoins* recebidos em sua carteira. O saldo fica disponível conforme as configurações da carteira, podendo ser liberado após uma ou mais confirmações, dependendo do nível de segurança desejado. Por fim, a transação fica registrada permanentemente na *blockchain*, não podendo ser alterada ou cancelada. Isso garante a transparência e a segurança do sistema, evitando fraudes como o gasto duplo (enviar uma cópia de *bitcoin*).

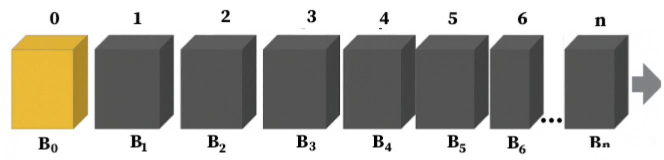
4.6 Bitcoin, sequência e progressão

No contexto da rede *Bitcoin*, os blocos podem ser compreendidos como elementos de uma sequência ordenada e encadeada no tempo. Cada bloco contém um conjunto de transações validadas, um carimbo de data/hora e um identificador único (o *hash*), além do *hash* do bloco anterior. Essa estrutura encadeada estabelece uma relação de dependência entre os blocos, garantindo a integridade da cadeia como um todo.

Sob o ponto de vista matemático, é possível interpretar os blocos como termos de uma sequência (B_n), onde cada B_n representa o n-ésimo bloco adicionado à *blockchain*. Essa sequência é crescente em relação ao tempo de inclusão na rede e ao número do bloco, iniciando com o bloco gênesis (B_0) e progredindo conforme novos blocos são minerados aproximadamente a cada 10 minutos.

Essa perspectiva permite aplicar conceitos matemáticos de sequências e progressões à análise da *blockchain*, como regularidade temporal, crescimento acumulado e dependência entre elementos consecutivos. Além disso, o estudo da sequência dos blocos pode oferecer subsídios para a compreensão do funcionamento da rede, da segurança proporcionada pela prova de trabalho (*Proof of Work*) e da resistência a ataques como a reorganização da cadeia. Assim, ao tratar os blocos como uma sequência matemática, estabelece-se uma ponte entre a tecnologia do *Bitcoin* e os conteúdos da matemática escolar, especialmente no ensino de funções, sequências e progressões. Na Figura 11, associamos os números dos blocos a uma sequência (B_0, B_1, B_2,..., B_n, $\ldots$).

Figura 11 – Associação entre blocos da rede bitcoin e uma sequência



Fonte: Elaborado pelo autor (2024)

4.6.1 A natureza infinita da sequência de blocos na rede Bitcoin

A *blockchain* do *Bitcoin* pode ser interpretada como uma sequência potencialmente infinita de blocos. Essa rede é estruturada por meio da adição contínua de novos blocos, que são minerados aproximadamente a cada 10 minutos. Cada bloco registra um conjunto de transações e referencia criptograficamente o bloco anterior, formando assim uma cadeia crescente e encadeada no tempo.

Do ponto de vista matemático, a sequência de blocos pode ser denotada por (B_n), onde B_0 representa o bloco gênese e B_n o n-ésimo bloco gerado. Em qualquer instante, o número de blocos já minerados é finito; contudo, não há um limite superior predefinido para a quantidade de blocos que podem ser criados no futuro, o que caracteriza a sequência como potencialmente infinita.

Assim, a rede *Bitcoin* pode ser compreendida como uma sequência infinita em construção, cujo crescimento contínuo depende apenas da manutenção de sua infraestrutura descentralizada e da participação ativa dos mineradores.

4.6.2 Número de transações por bloco e sua representação didática

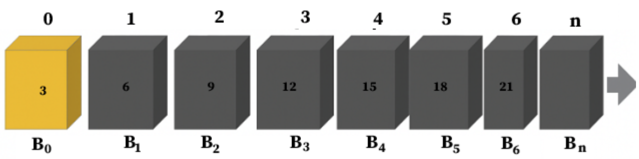
Cada bloco da rede *Bitcoin* contém um conjunto de transações válidas que foram agrupadas e registradas pelos mineradores. O número de transações incluídas em cada bloco varia conforme diversos fatores, como a demanda de uso da rede, o tamanho individual das transações e o limite máximo de dados permitidos por bloco (em torno de 1 MB na rede principal).

Do ponto de vista matemático, a quantidade de transações por bloco não segue uma regularidade numérica fixa e, por isso, não pode ser descrita formalmente como uma sequência aritmética ou geométrica. Mais especificamente, essa quantidade não caracteriza uma **progressão aritmética**, pois não há uma razão comum constante entre os termos sucessivos. Em vez disso, a variação no número de transações é aleatória e depende das condições dinâmicas da rede no momento em que cada bloco é minerado.

No entanto, do ponto de vista didático, essa irregularidade pode ser suavizada por meio de representações ilustrativas. Para fins de ensino de progressões e sequências, por exemplo, pode-se utilizar um modelo simplificado em que o número de transações por bloco cresça ou decresça de forma regular, como em uma progressão aritmética ou geométrica hipotética. Essa abordagem não busca refletir com precisão o funcionamento real da rede, mas sim criar um contexto significativo no qual os estudantes possam aplicar conceitos matemáticos formais em um ambiente inspirado em aplicações tecnológicas contemporâneas, como a *blockchain*.

Dessa forma, a rede *Bitcoin* pode servir como uma ponte entre a matemática e o mundo digital, permitindo a elaboração de atividades didáticas contextualizadas que estimulem o pensamento lógico e a modelagem matemática, mesmo que isso envolva abstrações que se afastam da realidade técnica. Na Figura 12, acrescentamos quantidades de transações a cada bloco, que vão aumentando e formando uma PA de razão 3, ou seja, no bloco B_0 possui 3 transações, B_1 possui 6 transações , B_2 possui 9 transações, e assim por diante.

Figura 12 – Quantidade de transações no bloco



Fonte: Elaborado pelo autor (2024)

Dentro desse contexto podemos destacar problemas como: Suponha que a rede *Bitcoin* comece com 300 transações no primeiro bloco. Se o número de transações diminui em 20 a cada bloco, quantas transações haverão no 10º bloco?

4.6.3 As unidades de bitcoin (BTC) representam uma Progressão geométrica?

No protocolo do *Bitcoin*, as unidades de bitcoin (BTC) geradas a cada ciclo de mineração representam uma progressão geométrica devido ao mecanismo conhecido como *halving* (redução pela metade), que ocorre aproximadamente a cada 210.000 blocos, ou cerca de quatro anos.

- **Mecanismo de halving:** A recompensa dada aos mineradores por adicionar um novo bloco à **blockchain** do *Bitcoin* começou em 50 *bitcoins* por bloco no lançamento da rede, em 2009. A cada 210.000 blocos minerados, essa recompensa é reduzida pela metade, ou seja, multiplicada por um fator constante $\alpha = \frac{1}{2}$.

- **Característica da progressão geométrica:** No caso do *Bitcoin*, a quantidade de bitcoins gerados em cada ciclo é dada por:

$$R_i = R_0 \times \left(\frac{1}{2}\right)^i,$$

onde:

- $R_0 = 50$ *bitcoins* (recompensa inicial);
- i é o número do ciclo de *halving* ($i = 0, 1, 2, \ldots$);
- $\frac{1}{2}$ é a razão da progressão geométrica; representando a redução pela metade da recompensa a cada ciclo.

Exemplo prático: Considere o seguinte problema:

- No ciclo $i = 0$, a recompensa é 50 BTC por bloco.
- No ciclo $i = 1$, a recompensa é $50 \times \frac{1}{2} = 25$ BTC.
- No ciclo $i = 2$, a recompensa é $25 \times \frac{1}{2} = 12,5$ BTC, e assim por diante.

A quantidade total de *bitcoin* que serão gerados ao longo do tempo é a soma dos termos dessa progressão geométrica multiplicada pelo número de blocos em cada ciclo (210.000 blocos). Como a razão $r = \frac{1}{2}$ é menor que 1, essa soma converge para um limite finito, que corresponde ao limite máximo total de *bitcoins* que existirão (aproximadamente 21 milhões).

4.6.4 Cálculo da soma total da oferta de bitcoins

O limite máximo de unidades de *bitcoins* foi estabelecido por seu criador, Satoshi Nakamoto, e está embutido no código-fonte da rede *Bitcoin*. Esse limite cria uma escassez semelhante à do ouro, o que ajuda a preservar o valor do *Bitcoin* ao evitar a inflação das moedas emitidas por banco central, que podem ser inflacionadas ilimitadamente pelos governos.

> Do dinheiro commodity material (gado, sal, ouro ou prata), o mundo evoluiu ao papel-moeda e à moeda escritural. A intangibilidade desta permitiu aos bancos a criação quase ilimitada de moeda, corroendo continuamente o poder de compra do dinheiro que usamos. A intangibilidade do Bitcoin, por outro lado, propiciou justamente o oposto; assegurou a escassez da moeda, a fim de preservar – e não corroer – o seu poder de compra. (ULRICH, 2014, p.77)

O limite resulta da estrutura do protocolo de mineração, que reduz pela metade a recompensa dos mineradores a cada 210 mil blocos (aproximadamente a cada quatro anos), começando com 50 BTC por bloco. Essa redução contínua, chamada de *halving*, faz com que a soma total das recompensas atinja exatamente 21 milhões ao longo do tempo.

Consideremos os seguintes dados para que possamos calcular a soma total de *bitcoins*:

- Recompensa inicial por bloco: $R_0 = 50$ *bitcoins*;
- Número de blocos por ciclo: $N = 210000$;
- Razão da progressão geométrica: $r = \frac{1}{2}$ (recompensa reduzida pela metade a cada ciclo);
- Número do ciclo: $i = 0, 1, 2, \ldots$.

Já recompensa por bloco no ciclo i é:

$$R_i = R_0 \times r^i = 50 \times \left(\frac{1}{2}\right)^i.$$

.

A quantidade total de *bitcoins* gerados no ciclo i é dada por:

$$Q_i = R_i \times N = 50 \times \left(\frac{1}{2}\right)^i \times 210000.$$

Assim, temos a seguinte expressão para a soma total de *bitcoins* gerados ao longo de todos os ciclos:

$$S = \sum_{i=0}^{\infty} Q_i = 210000 \times 50 \times \sum_{i=0}^{\infty} \left(\frac{1}{2}\right)^i.$$

Como $0 < r = \frac{1}{2} < 1$, a soma da série geométrica infinita é:

$$\sum_{i=0}^{\infty} r^i = \frac{1}{1-r} = \frac{1}{1-\frac{1}{2}} = 2.$$

Logo,

$$S = 210000 \times 50 \times 2 = 210000 \times 100 = 21000000.$$

Dessa forma, a soma total da oferta de *bitcoins* gerados pelo protocolo é limitada a 21 milhões de unidades, devido à convergência da progressão geométrica decrescente da recompensa por bloco a cada ciclo de *halving*.

5 Relato de experiência da sequências didática

Neste capítulo, apresentamos um relato de experiência sobre a aplicação de uma sequência didática proposta como recurso educacional, vinculado a este trabalho, disponível no site eduCapes, Apêndice B. Trata-se de uma sequência didática que integra o ensino de sequências e progressões, utilizando um recurso tecnológico atual: a rede *Bitcoin*, que pode ser visualizada no site *mempool*, disponível em <https://mempool.space/pt/>. Nessa abordagem, são trabalhados os conceitos de sequências e progressões. A sequência foi composta por sete encontros planejados para promover o letramento matemático e o pensamento crítico, conforme diretrizes da BNCC e da Paraíba (2021).

Nossa proposta visa aproximar o conteúdo matemático da realidade dos estudantes, utilizando a rede do *Bitcoin* como associação concreta para o estudo de padrões numéricos.

Segundo Zabala (1998), uma sequência didática é um conjunto estruturado e ordenado de atividades com objetivos definidos, tanto pelos professores quanto pelos alunos. É amplamente reconhecido que o conhecimento matemático desempenha um papel fundamental na formação dos estudantes da Educação Infantil, do Ensino Fundamental e do Ensino Médio. A matemática fornece ferramentas essenciais para a compreensão e a atuação crítica na sociedade contemporânea, contribuindo para que o aluno se torne um cidadão consciente, participativo e responsável no contexto em que está inserido.

> A maneira de configurar as sequências de atividades é um dos traços mais claros que determinam as características diferenciais da prática educativa. Desde o modelo mais tradicional de "aula magistral" (com a seqüência: exposição, estudos sobre apontamentos ou manual, prova, qualificação) até o método de "projetos de trabalho global" (escolha do tema, planejamento, pesquisa e processamento da informação, índice, dossiê de síntese, avaliação), podemos ver que todos têm como elementos identificadores as atividades que os compõem, mas que adquirem personalidade diferencial segundo o modo como se organizam e articulam em seqüências ordenadas (ZABALA, 1998, pag.26).

Cabe destacar que a Educação Básica, em todas as suas etapas, tem como compromisso a promoção do letramento matemático, que envolve a capacidade de resolver problemas, mobilizar conhecimentos, desenvolver habilidades e competências — tanto gerais quanto específicas. Esses processos estão orientados por documentos normativos como a BNCC e o Currículo da Rede Estadual da Paraíba Paraíba (2021). Tais diretrizes reforçam que as aprendizagens previstas devem ser garantidas a todos os estudantes, independentemente de sua localização geográfica ou da instituição em que estudam. Além disso, é importante ressaltar o papel da tecnologia no processo de ensino da matemática.

> O datashow e os tablets diversificaram as formas de apresentação de conteúdo a partir da projeção de imagens e vídeos. Outros recursos digitais adotados pelos educadores foram a plataforma IBGE Educa e o aplicativo Rei da Matemática, que possui interface divertida e oferece exercícios com diferentes níveis de dificuldade (CORREA; TANIGUTI; FERREIRA, 2021, p.51)

O uso de ferramentas computacionais voltadas à análise de dados e à visualização gráfica pode tornar as aulas mais atrativas, interativas e eficazes. Diante disso, desenvolvemos uma sequência didática composta por sete encontros e aplicado em uma turma de 1º ano do Ensino Médio da Escola Estadual de Ensino Fundamental e Médio Reitor Edvaldo do Ó na cidade de Campina Grande-PB, as quais planejamos os objetivos e procedimentos necessários para alcançá-los. Sendo assim, a cada encontro apresentamos a unidade temática, modalidade/nível de ensino, objetos de conhecimento, habilidades, objetivos/expectativas de aprendizagem, estratégia de ensino, materiais utilizados e a duração das atividades em cada encontro da sequência desenvolvida.

Para estes encontros, utilizamos alguns recursos que consideramos fundamentais para ensino/aprendizagem do aluno, como a rede do *bitcoin*, a associação dos blocos da rede com conceitos matemáticos e recorremos a apresentação dos blocos aos alunos por meio do site <https://mempool.space/pt/> e uma breve dinâmica de criptografia e descriptografia com o objetivo de tornar lúdica essa abordagem. As fontes principais que usamos foram o livro Dinheiro na era Digital de Ulrich (2014), Nakamoto (2008), Carvalho e Morgado (2017), Marques (2019) e a BNCC.

No ambiente da *mempool*, é possível visualizar listas ordenadas de blocos e números de transações nesse bloco, o que permite associar esses blocos a sequências matemáticas e as transações a progressões. Ao trazer esse recurso tecnológico para a sala de aula, o professor tem a oportunidade de apresentar os conceitos de sequência, progressão aritmética e progressão geométrica de maneira aplicada, interativa e atual, despertando o interesse dos estudantes. O uso de ferramentas como o site mempool.space permite a observação em tempo real dessas sequências, promovendo o conhecimento matemático por meio de dados reais, o que está em conformidade com os princípios da BNCC, que orienta para o uso de situações contextualizadas e recursos tecnológicos no processo de ensino-aprendizagem da matemática.

Além disso, ao associar conteúdos abstratos da matemática com tecnologias emergentes como o *blockchain* e o *Bitcoin*, favorece-se uma aprendizagem significativa, conectando a matemática escolar a temas contemporâneos e fomentando o pensamento crítico e a interdisciplinaridade. A utilização desse recurso *blockchain* teve o objetivo pedagógico e visual, nossa intenção foi apenas de apresentar o funcionamento da rede e não fazermos algum investimento ou utilizar *software* para fazer as transações, pois, isso demandaria muito tempo e outros conhecimentos.

É comum a nós professores associarmos a ideia de recurso tecnológico a um instrumento motivacional, mas na verdade é mais do que isso: ela traz importância da tecnologia na educação para promover a aprendizagem significativa e preparar os alunos para o uso crítico e responsável das ferramentas digitais como destaca a Brasil (2017), que enfatiza o uso de tecnologias de forma integrada ao currículo, favorecendo o desenvolvimento de competências digitais, como a pesquisa, a comunicação e a resolução de problemas. Acreditamos que por meio do uso de recursos tecnológicos podemos obter resultados mais positivos com relação ao ensino. Marques (2019) ainda reforça a ideia de que é possível ensinar matemática de forma contextualizada e aplicável sem atrapalhar o entendimento dos conceitos formais, definições e propriedades.

5.1 Relato de experiência

Neste relato de experiência documentamos o passo a passo na execução das ações da sequência didática no ensino de sequências numéricas e progressões com a tecnologia da cadeia de blocos da rede *bitcoin*, conforme o recurso educacional vinculado a esse trabalho. A sequência didática foi aplicada pelo próprio autor durante suas aulas de Matemática na Escola Estadual de Ensino Fundamental e Médio Reitor Edvaldo do Ó, localizada na cidade de Campina Grande, Paraíba, junto à turma do 1º A ano do Ensino Médio.

A sequência didática foi organizada conforme o Quadro 3. Aplicadas nas aulas do componente curricular de matemática do ensino médio para o 1° ano A regular com duração média de 2h/a para cada encontro com carga horária total de 12 horas-aulas. Vale salientar que o tempo pedagógico proposto nesta sequência didática pode e deve ser ajustado conforme as especificidades de cada turma. A flexibilidade na gestão do tempo é essencial para atender às diferentes realidades escolares, considerando o ritmo de aprendizagem dos alunos, suas experiências prévias e o nível de familiaridade com os conteúdos abordados.

Quadro 3 – Organização dos Encontros

Organização dos Encontros	
Data	**Conteúdo/Atividades**
04/11/2024	Introdução à sequências numéricas, elementos de uma sequência, recorrência e termo geral.
07/11/2024	Introdução à rede Bitcoin, mempool do Bitcoin e como ela é formada por uma sequência de blocos e transações.
11/11/2024	Progressão Aritmética, classificação da PA, termo geral da PA e PA na rede Bitcoin.
12/11/2024	Soma da Progressão Aritmética.
14/11/2024	Progressão Geométrica, classificação, termo geral da PG. Recompensas em BTC a cada bloco formam uma PG.
18/11/2024	Soma dos termos de uma PG finita, soma dos termos de uma PG infinita, soma de unidades de BTC por ciclos; limite total de BTC possível de ser minerado.
19/11/2024	Questionário de avaliação da metodologia utilizada em sala de aula.

Fonte: Elaborado pelo próprio autor.

A seguir descrevemos cada encontro, seguindo a metodologia estabelecida na sequência didática. Cada parte inclui as atividades realizadas, as discussões promovidas e os resultados alcançados.

5.1.1 Encontro 1: Introdução à sequências numéricas, elementos de uma sequência, recorrência e termo geral

No primeiro encontro, participaram 30 (trinta) alunos da turma. Antes de darmos início à aplicação da sequência didática, foi realizada uma breve apresentação da proposta, com o objetivo de contextualizar os estudantes quanto à organização dos sete encontros planejados.

No momento 1, apresentamos a sequência de Fibonacci. Durante a aula expositiva, o tema foi introduzido por meio de uma explicação sobre sequências numéricas, adotando-se a proposta de utilizar o termo lista para facilitar a compreensão dos estudantes. Como exemplo inicial, foi apresentada a sequência de Fibonacci. Essa sequência foi escrita no quadro e os alunos foram divididos em grupos, conforme a Figura 13, para discutir e tentar prever o próximo termo da sequência. Ainda para facilitar a busca pelo próximo termo da sequência de Fibonacci os alunos foram incentivados a encontrar a lógica por trás da sequência. Qual é o padrão de formação da sequência?

Figura 13 – Alunos do 1° ano em Grupo

Fonte: Elaborado pelo próprio autor.

Cada grupo apresentou suas descobertas e a regra para encontrar o próximo termo da sequência, alguns alunos chegaram à compreensão rapidamente de que o próximo termo é a soma dos dois termos anteriores ($1 + 1 = 2$, $1 + 2 = 3$, etc.) e socializaram com os demais. Os alunos demonstraram uma boa compreensão da regra de formação da sequência de Fibonacci, desenvolvendo habilidades de raciocínio lógico e trabalho em equipe. Nos próximos momentos do encontro apresentamos os conceitos de sequência e sequência numérica de acordo com a proposta de sequência didática, definição formal de sequência, sequência numérica, sequência numérica finita e infinita, lei de formação de uma sequência, recorrência e termo geral de uma sequência.

A aplicação desse primeiro encontro ocorreu de maneira bastante produtiva, com participação ativa e engajada pela maior parte dos estudantes. O desafio de identificar o padrão da sequência de Fibonacci despertou nos estudantes a curiosidade de reconhecer regularidades e compreender o padrão lógico nessa sequência. As expectativas de aprendizagem foram alcançadas, visto que os alunos compreenderam os conceitos introdutórios de sequência numérica e foram capazes de identificar padrões em sequência numéricas e apresentar justificativas coerentes. Um dos momentos mais significativos foi a socialização das conclusões entre os grupos, em que os próprios alunos verbalizaram, de forma clara, a regra de formação da sequência.

5.1.2 Encontro 2: Introdução à rede *Bitcoin*, *mempool* e como ela é formada por uma sequência de blocos e transações.

Nesse encontro, estavam presentes 32 alunos. No momento 1 introduzimos a rede *Bitcoin* e iniciamos a aula com um debate sobre "O que é o Bitcoin?". Muitos alunos expressaram incertezas sobre o tema; outros, no entanto, afirmaram que se trata de uma moeda digital, um investimento ou uma criptomoeda. Alguns já possuíam conhecimento mais aprofundado, como o entendimento de que se trata de uma moeda descentralizada, que não necessita de um banco central para ser emitida.

Em seguida explicamos o que é *Bitcoin* e como funciona sua tecnologia *blockchain*, utilizando recursos visuais como slides e o site mempool.space, seguindo a metodologia descrita na sequência didática, conforme a Figura 14. Aqui também chamamos a atenção para o risco de volatilidade de preço e golpes envolvendo o nome *Bitcoin* para atrair investidores.

Figura 14 – Apresentação da rede Bitcoin

Fonte: Elaborado pelo próprio autor.

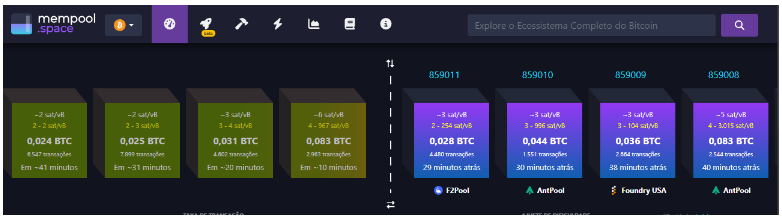
Ainda nesse primeiro momento, fizemos o questionamento se a rede *Bitcoin* é uma sequência. Seguimos com a proposta da sequência didática, buscando apresentar de forma lúdica e acessível os conceitos de criptografia na rede *Bitcoin*, o funcionamento da rede e o processo de transação e validação das informações nos blocos. Para isso os alunos foram organizados em filas, e cada fila representava uma cadeia de blocos (*blockchain*), permitindo uma simulação prática do funcionamento da tecnologia.

A atividade consistiu no envio de mensagens criptografadas pelo professor até o último aluno de cada fila, simulando a propagação de dados na rede. Apenas o professor e o último aluno de cada fila tinham conhecimento prévio do algoritmo utilizado para criptografar e descriptografar as mensagens. Optamos por um algoritmo simples de substituição, no qual cada número era associado a uma letra do alfabeto (por exemplo, 1 = A, 2 = B, ..., 26 = Z). As mensagens eram escritas utilizando apenas os números correspondentes às letras, e o último aluno da fila tinha a responsabilidade de decodificá-las corretamente e anunciá-las ao restante da turma. Com isso, buscou-se representar de maneira concreta a descentralização e o encadeamento de informações presente na rede do *Bitcoin*, bem como introduzir os estudantes ao conceito de criptografia de forma acessível. Quando o último aluno revelava a mensagem, os alunos sem saber como aqueles números poderiam transmitir uma mensagem, perguntavam como é possível: "Como assim?"

Essa abordagem despertou grande interesse entre os alunos e facilitou a compreensão do conteúdo, ao estabelecer conexões entre os conceitos matemáticos trabalhados e uma aplicação prática inspirada no universo digital e tecnológico do *Bitcoin*.

No Momento 2, resolvemos os três problemas que correlacionam a rede do *Bitcoin* à sequência e progressão. No primeiro problema, estudou-se a natureza da rede com uma sequência pela seguinte pergunta: "A rede *Bitcoin* é uma sequência?". Nesse problema, todos os alunos destacaram rapidamente a associação dos blocos a elementos de uma lista e confirmaram que se trata de uma sequência. O segundo problema foi norteado pela pergunta: "A rede *Bitcoin* é uma sequência finita ou infinita de blocos?". Aqui faço um relato que alguns alunos tinham curiosidade sobre infinitude de algo, se era algo que continuava? E observando a *mempool*, foi possível ver uma sequência de blocos contínua pelo site https://mempool.space/pt/ como na Figura 15.

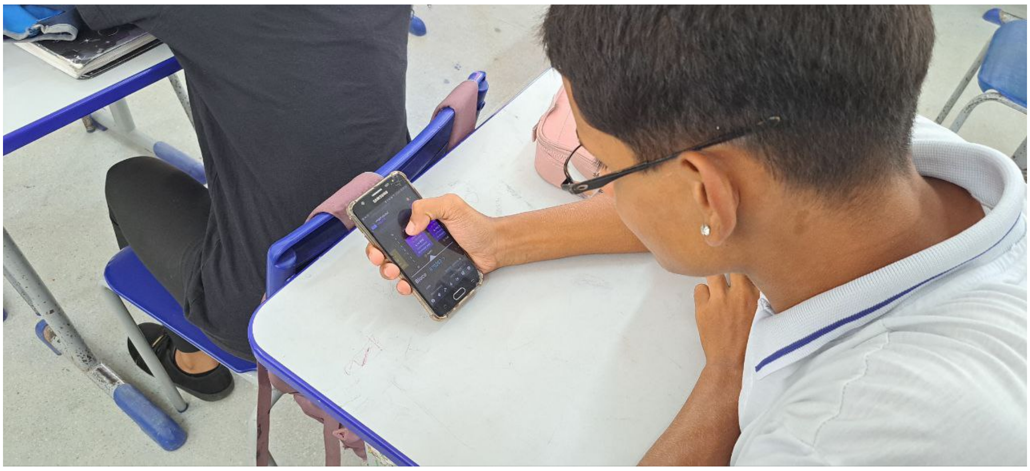
Figura 15 – Mempool do bitcoin



Fonte: Elaborado pelo próprio autor.

Para o terceiro e último problema, vimos que a rede do *Bitcoin* recompensa o minerador a cada bloco e, a cada ciclo de 210 mil blocos, essa recompensa é reduzida pela metade. O primeiro ciclo recompensava o minerador com 50 BTC. O enunciado do terceiro problema, então, foi: "Qual será a recompensa por bloco minerado após 4 ciclos?". Nesse problema levou mais tempo para a resolução, entretanto, a maior parte dos alunos permaneciam interessados em resolver o problema visto que era possível verificar na rede o resultado final, os alunos chegaram a conclusão que bastava dividir 50 pela metade 4 vezes seguidas e assim chegariam ao resultado. Após os alunos chegarem ao resultado de 3,125, pedimos aos alunos que tinham celular e internet nesse momento que consultasse o site indicado, Figura 16.

Figura 16 – Aluno observando a mempool do Bitcoin



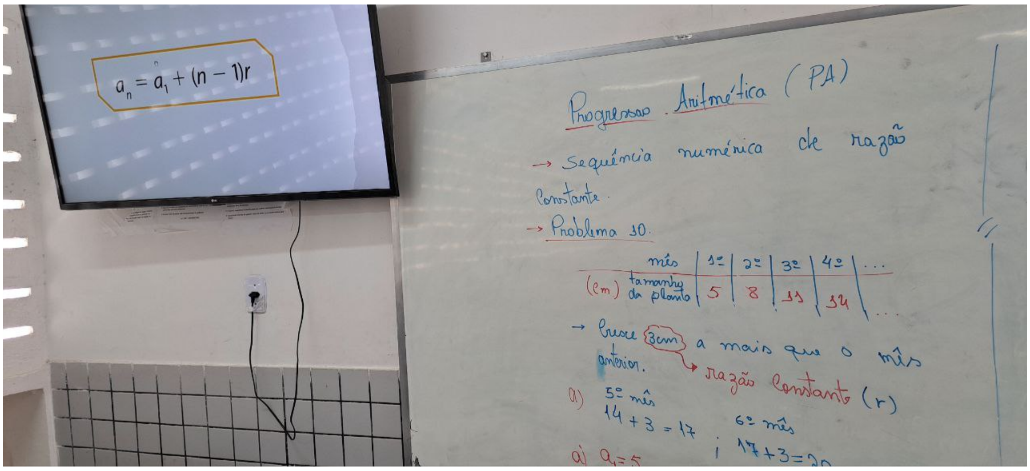
Fonte: Elaborado pelo próprio autor.

A aplicação desse segundo encontro revelou-se especialmente rica em curiosidade dos alunos. A introdução ao tema *Bitcoin* despertou a curiosidade, que, embora apresentassem níveis distintos de familiaridade com o assunto, participaram ativamente das discussões iniciais. A simulação prática da *blockchain*, com o site mempool.space e por meio de filas representando cadeias de blocos e mensagens criptografadas, promoveu um ambiente lúdico e colaborativo, favorecendo a compreensão dos conceitos da rede da criptografia. A proposta gerou questionamentos espontâneos por parte dos estudantes, evidenciando envolvimento cognitivo e interesse genuíno. No momento em que a rede *Bitcoin* foi associada a uma sequência, os alunos estabeleceram conexões com o conteúdo matemático, identificando regularidades e explorando o conceito de infinitude. A resolução dos problemas, sobretudo o que envolvia a recompensa por blocos, foi mais desafiadora, mas provocou empenho coletivo, com alunos recorrendo à verificação prática no site mempool.space. Esses aspectos reforçam a eficácia da abordagem contextualizada e interdisciplinar adotada na sequência didática.

5.1.3 Encontro 3: Progressão Aritmética, classificação da PA, termo geral da PA e PA na rede Bitcoin.

Nesse encontro estavam presentes 23 alunos. No primeiro momento iniciamos a aula expondo o problema de progressão aritmética proposta na sequência didática, além de apresentá-lo em *slides*, e fizemos uma tabela esquematizando o problema no quadro, conforme a Figura 17. Os alunos trabalharam para resolver o problema sobre o crescimento de uma planta e após algumas tentativas conseguiram chegar no objetivo da pergunta. Em seguida, apresentamos o conceito de progressão aritmética, termo geral e exemplos como descrito na proposta da sequência didática.

Figura 17 – Problema escrito no quadro



Fonte: Elaborado pelo próprio autor.

No segundo momento resolvemos os 3 (três) problemas com progressão aritmética e a *blockchain* do *Bitcoin* propostas na sequência didática. Os blocos da rede *Bitcoin* formam uma PA? Se sim, qual é a razão? Como estávamos observando esse problema a partir da *mempool* iniciando do bloco gêneses, ao observar os números acima do bloco, os alunos descreveram que sim, era uma PA e sua razão era um.

Do bloco 420100 ao bloco 420104, as transações formam uma PA? Se sim, qual a razão? Ainda na *mempool* mostramos como encontrar o bloco 420100 e a partir dele verificar se as transações seguintes formam uma PA, como as transações não fizeram uma sequência lógica a conclusão foi que não é uma PA.

Suponha que a rede *Bitcoin* comece com 300 transações no primeiro bloco. Se o número de transações diminui em 20 a cada bloco, quantas transações haverão no 10º bloco? A dificuldade inicial dos alunos foi associar o problema a PA, mas nas tentativas, a maior parte dos alunos chegaram a conclusão que bastava diminuir 20 transações seguidas, partindo de 300 e assim chegariam a solução.

Além dessa resolução feita pelos alunos, mostramos que seria possível resolver o problema e encontrar a quantidade de transações no bloco utilizando o termo geral de PA, através do seguintes cálculos: : o termo geral da PA é

$$a_n = a_1 + (n - 1)r;$$

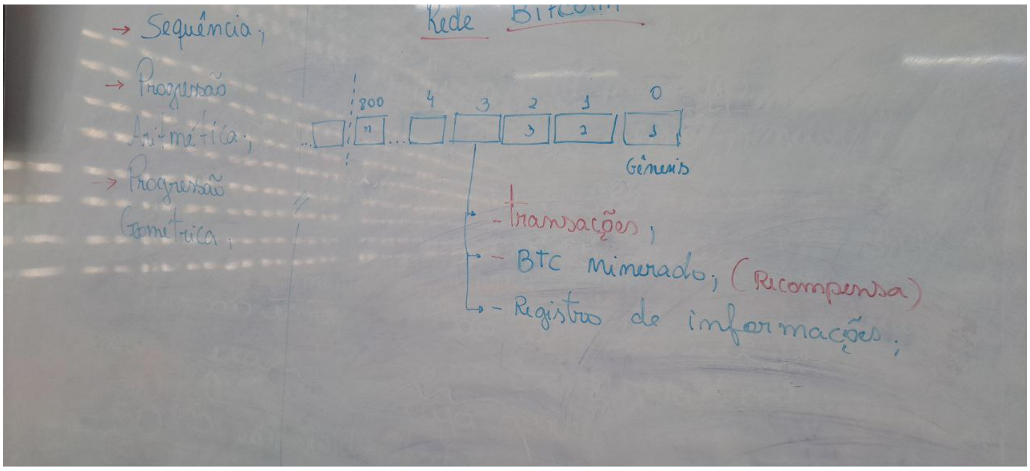
considerando $a_1 = 300$, $r = -20$, calculamos o valor correspondente ao 10º bloco ($n = 10$):

$$300 - 20 \times (10 - 1) = 300 - 20 \times 9 = 300 - 180 = 120;$$

portanto, no 10º bloco haverá **120 transações**.

Desenhamos a representação dos blocos e quantidades de transação, no quadro, para facilitar o raciocínio e resolução dos problemas, Figura 18.

Figura 18 – Blocos da rede bitcoin desenhadas no quadro



Fonte: Elaborado pelo próprio autor.

5.1.4 Encontro 4: Soma da Progressão Aritmética.

Nesse encontro estavam presentes 32 alunos e durou apenas $1h/a$. No primeiro momento iniciamos a aula relembrando os conceitos de PA e, em seguida, foi proposta aos alunos uma atividade envolvendo a soma dos números naturais de 1 até 100, com o objetivo de estimular o raciocínio lógico e a percepção de padrões nas sequências numéricas. Sem recorrer, inicialmente, à fórmula da soma de uma progressão aritmética, os estudantes foram incentivados a explorar estratégias próprias de contagem e agrupamento.

Após alguns minutos, introduzimos a dica de somar o primeiro número com o último, o segundo com o penúltimo, e assim sucessivamente e finalmente alguns alunos conseguiram chegar ao objetivo. Em seguida, introduzimos a fórmula da soma da progressão aritmética e pedimos que os alunos aplicassem no mesmo problema chegando a mesma conclusão.

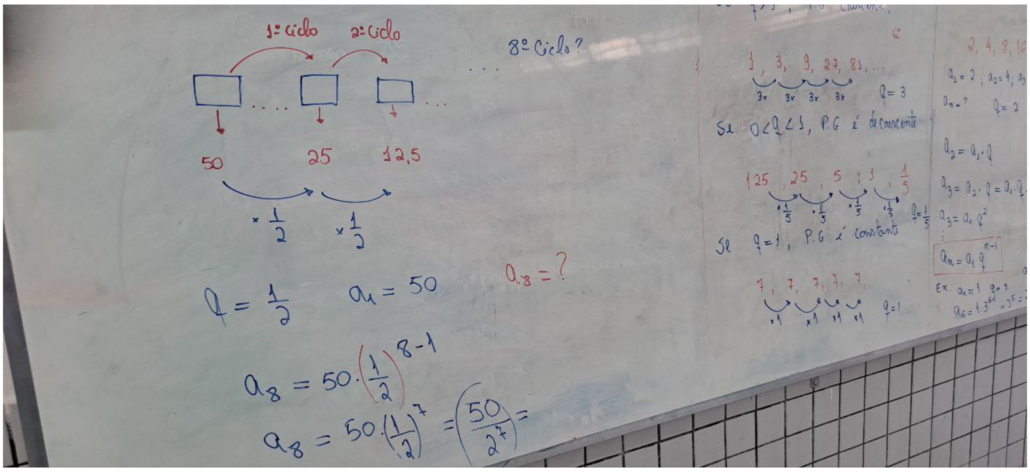
Os alunos conseguiram compreender que a soma de termos de uma progressão aritmética pode ser obtida tanto pela percepção do padrão de agrupamento dos números quanto pela aplicação da fórmula correspondente, reconhecendo que ambas as estratégias conduzem ao mesmo resultado e consolidando, assim, a compreensão do conceito.

5.1.5 Encontro 5: Progressão Geométrica, classificação, termo geral da PG, recompensas em BTC a cada bloco formam uma PG.

Nesse encontro estavam presentes 27 alunos. Iniciamos a aula com um problema de progressão geométrica proposta na sequência didática e os alunos foram desafiados a encontrar os próximos valores de uma sequência de economia no qual o valor dobrava a cada mês, sem utilizar, inicialmente, a fórmula da progressão geométrica. Após alguns minutos alguns alunos conseguiram resolver o problema chegando ao objetivo de encontrar os próximos valores. Em seguida explicamos o conceito de progressão geométrica e a razão q que define a diferença entre os termos.

No segundo momento resolvemos os 3 (três) problemas com progressão geométrica e a *blockchain* do *Bitcoin* propostas na sequência didática. Para facilitar a relação entre o problema proposto e os blocos do *Bitcoin*, além de ilustrarmos com a própria rede do *Bitcoin* também desenhamos a associação da progressão com os blocos, transações e as unidades de *Bitcoin* (BTC) recebidas pelos minerados, Figura 19 .

Figura 19 – Desenho da rede Bitcoin no quadro



Fonte: Elaborado pelo próprio autor.

O primeiro ciclo recompensava o minerador em 50 BTC, em 8 ciclos, qual a recompensa por bloco minerado? Nesse problema relembramos algumas informação para os alunos, como a redução pela metade de recompensas de BTC a cada ciclo. E após essa informação, a maior parte dos alunos concluíram que bastava dividir 50 oito vezes seguidas e encontrariam o resultado. Questionamos se existia outra maneira mais rápida de resolver e alguns alunos apontaram a possibilidade de utilizar a fórmula de termo geral da PG. Apresentamos a seguinte resolução:

A recompensa por bloco minerado na rede *Bitcoin* forma uma progressão geométrica, onde:

- O primeiro termo (a) é 50 BTC (recompensa do primeiro ciclo);
- A razão (q) é $\frac{1}{2}$ (a recompensa é reduzida pela metade a cada ciclo).

O termo geral de uma PG é dado pela fórmula:

$$a_n = a \cdot q^{n-1}.$$

Substituindo a e q temos,

$$a_n = 50 \cdot \left(\frac{1}{2}\right)^{n-1}.$$

Para determinar a recompensa após 8 ciclos ($n = 8$), basta fazermos,

$$a_8 = 50 \cdot \left(\frac{1}{2}\right)^{8-1} = 50 \cdot \left(\frac{1}{2}\right)^{7} = 50 \cdot \frac{1}{128} = \frac{50}{128} \approx 0.390625 \text{ BTC}.$$

Portanto, a recompensa por bloco minerado após 8 ciclos é aproximadamente **0.39 BTC**.

O primeiro ciclo recompensava o minerador em 50 BTC, em quantos ciclos a recompensa por bloco será de 3,125 BTC? Novamente a primeira tentativa dos alunos foi dividir o 50 sucessivas vezes até chegar em 3,125 e assim verificaram que se passavam 5 ciclos. Em seguida, mostramos que era possível resolver o problema utilizando a fórmula da PG, conforme a seguir.

O termo geral de uma PG é dado pela fórmula:

$$a_n = a \cdot q^{n-1}.$$

Substituindo a e q temos,

$$a_n = 50 \cdot \left(\frac{1}{2}\right)^{n-1}.$$

Queremos encontrar o valor de n quando $a_n = 3,125$ BTC, então

$$3,125 = 50 \cdot \left(\frac{1}{2}\right)^{n-1}.$$

Dividindo ambos os lados por 50, encontramos

$$\frac{3,125}{50} = \left(\frac{1}{2}\right)^{n-1} \Rightarrow 0,0625 = \left(\frac{1}{2}\right)^{n-1}.$$

Sabemos que $0,0625 = \left(\frac{1}{2}\right)^4$, logo:

$$\left(\frac{1}{2}\right)^{n-1} = \left(\frac{1}{2}\right)^{4}.$$

Igualando os expoentes:

$$n - 1 = 4 \Rightarrow n = 5.$$

Assim, a recompensa por bloco será de **3,125 BTC** no **5º ciclo**.

O primeiro ciclo recompensava o minerador em 50 BTC e 210 mil blocos são processados em aproximadamente 4 anos. Em quantos anos a recompensa por bloco minerado será de 6,25 BTC? Como os alunos já tinham dividido 50 cinco vezes seguidas, na quarta vez encontraram 6,25, então chegaram a conclusão que bastava multiplicar 4 ciclos por 4 anos e chegariam em 16 anos.

5.1.6 Encontro 6: Soma dos termos de uma PG finita, soma dos termos de uma PG infinita, soma de unidades de BTC por ciclos; limite total de BTC possível de ser minerado.

Nesse encontro estavam presentes 27 alunos. Iniciamos a aula revisando os conceitos de progressão geométrica e informações sobre a rede do *Bitcoin*, os quais foram utilizados para resolver problemas posteriores. Em um primeiro momento, iniciamos com o problema proposto na sequência didática (Emerson está planejando uma série de investimentos em renda fixa e decide fazer um investimento que segue uma progressão geométrica. Ele começará investindo R$ 1.000,00 no primeiro mês e, a cada mês, ele irá dobrar o valor investido no mês anterior. Qual é a soma total que Emerson investirá ao final dos 6 meses?). Tínhamos o objetivo de que os alunos chegassem no valor da soma sem utilizar a fórmula que foi apresentada posteriormente. Após os alunos chegarem a conclusão da soma, seguindo a proposta da sequência didática, apresentamos as fórmulas da soma da progressão geométrica finita e infinita.

No segundo momento, resolvemos 2 (dois) problemas sobre soma de progressão geométrica e, da mesma maneira que ilustramos os problemas do Encontro 05, ilustramos no quadro com desenhos da cadeia de blocos e o site mempool.space do *Bitcoin* para associar a progressão geométricas com as unidades de *bitcoin* (BTC) e as transações no bloco.

O primeiro ciclo recompensava o minerador em 50 BTC e 210 mil blocos são processados em aproximadamente 4 anos. (1) Com base no texto, resolva as seguintes perguntas: (a) Em dois ciclos quantos BTC terão sido minerados? (b) Em 4 ciclos qual o total de BTC minerado? No item (a) os alunos conseguiram encontrar facilmente a solução multiplicando 50 vezes 210 mil e somando a metade da multiplicação de 50 vezes 210 mil, já no item (b) tiveram bastante dificuldade para pensar em uma solução, mas chegaram à mesma conclusão que bastava somar e dividir pela metade, 4 vezes e multiplicar por 210 mil. Em seguida, apresentamos a maneira de resolver utilizando a fórmula da soma de termos da PG finita. Agora usamos a fórmula da soma nos quatro primeiros termos da PG:

$$S_4 = a_1 \cdot \left(\frac{1-q^4}{1-q} \right),$$

onde:

- $a_1 = 50$ BTC;
- $n = 210.000$;
- $q = \frac{1}{2}$.

Substituindo esses valores:

$$\begin{aligned} S_4 = &\ 50 \times 210.000 \times \left(\frac{1 - \left(\frac{1}{2}\right)^4}{1 - \frac{1}{2}} \right) \\ = &\ 50 \times 210.000 \times \left(\frac{1 - \frac{1}{16}}{\frac{1}{2}} \right) \\ = &\ 50 \times 210.000 \times \left(\frac{\frac{15}{16}}{\frac{1}{2}} \right) \\ = &\ 50 \times 210.000 \times \left(\frac{15}{16} \times 2 \right) \\ = &\ 50 \times 210.000 \times \frac{30}{16} \\ = &\ 50 \times 210.000 \times 1{,}875 = 19.687{,}500 \text{ BTC}. \end{aligned}$$

Portanto, o total minerado após 4 ciclos será de **19.687,500 BTC**.

5.1.7 Encontro 7: Questionário de avaliação da metodologia utilizada em sala de aula.

Nesse encontro estavam presentes 25 alunos e teve uma duração de $1h/a$. Aplicamos um questionário impresso para que os alunos pudessem responder. Tínhamos o objetivo de obter as opiniões dos alunos participantes da sequência didática utilizando a cadeia de blocos da rede *Bitcoin* no ensino de sequências e progressões realizada nas aulas de matemática pelo professor Emerson Rodrigues Alves por meio de um questionário no modelo ARCS (Atenção, Relevância, Confiança e Satisfação). Essa análise detalhada será tratada na Seção 5.2.

Ao longo das aplicações da sequência didática pudemos notar que a maior parte dos alunos se mostraram mais engajados e motivados ao aprender sobre sequências numéricas e progressões. A utilização de recursos como o site mempool.space e atividades associadas aos blocos do *Bitcoin*, facilitou a visualização e compreensão dos conceitos de maneira mais concreta, permitindo que os estudantes desenvolvessem habilidades de raciocínio lógico e trabalho em equipe.

Além disso, a proposta atendeu aos princípios da Base Nacional Comum Curricular, que enfatiza a importância de situações contextualizadas e o uso de tecnologias no processo de ensino-aprendizagem. A experiência também destaca a relevância de preparar os alunos para um uso crítico e responsável das ferramentas digitais, alinhando-se às necessidades do século XXI. Os *feedbacks* obtidos por meio do questionário aplicado ao final da sequência didática evidenciam a eficácia da metodologia utilizada, detalhada na Seção 5.2.

5.2 Aplicação e análise do questionário com base no modelo ARCS

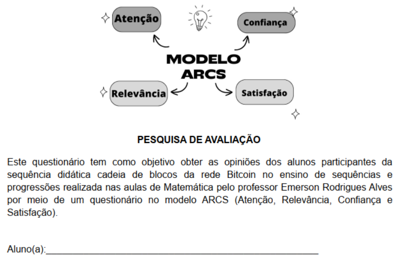
Nesta seção, apresentamos a análise de um questionário aplicado à turma do 1º ano A, composta por 32 alunos. No entanto, apenas 25 participaram da aplicação, uma vez que nem todos estavam presentes no último encontro. Essa pesquisa tem o objetivo de avaliar o nível de motivação proporcionado pela metodologia adotada durante a sequência didática sobre sequências e progressões, que teve como tema central a cadeia de blocos do *Bitcoin*. A coleta de dados foi realizada por meio de um questionário baseado no modelo ARCS, desenvolvido por John Keller (professor emérito da Florida State University) em 1983, modelo amplamente reconhecido e validado na área de educação. O objetivo do modelo ARCS é oferecer uma estrutura sistemática e eficaz para o design de ambientes de aprendizagem mais motivadores, visando aumentar o engajamento dos estudantes e promover um envolvimento mais profundo com o conteúdo. O modelo é estruturado em quatro componentes principais: Atenção, Relevância, Confiança e Satisfação.

O questionário foi aplicado à turma após a conclusão da sequência didática, que explorou conceitos matemáticos como progressões aritméticas e geométricas, além de sequências numéricas, utilizando como fio condutor o funcionamento da *blockchain* do *Bitcoin*. Durante as atividades, os alunos realizaram tarefas como calcular a quantidade de blocos minerados ao longo de determinados intervalos de tempo, analisar o crescimento de transações na rede em forma de progressões e interpretar a emissão de *bitcoins* em blocos de recompensa decrescentes, criando assim conexões entre os conceitos matemáticos e essa tecnologia.

O instrumento de avaliação continha um total de doze questões, distribuídas de forma a contemplar os quatro componentes do modelo ARCS: três questões relacionadas à atenção, três à relevância, três à confiança e três à satisfação. As perguntas buscaram identificar, por exemplo, se o uso do contexto *Bitcoin* chamou a atenção dos alunos para o conteúdo matemático, se os estudantes perceberam a relevância dos conceitos de sequências e progressões aplicados a um tema contemporâneo, se sentiram confiança ao realizar as atividades propostas e se ficaram satisfeitos por participar de uma experiência didática diferenciada.

O questionário, Figura 20, completo encontra-se no Apêndice A. Como o questionário foi aplicado de forma impressa, os dados coletados foram acrescentados na planilha eletrônica *calc* para serem gerados os gráficos apresentados a seguir.

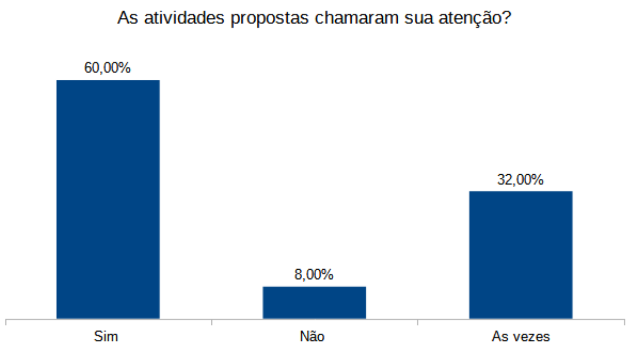
Figura 20 – Questionário Baseado em ARCS



Fonte: Elaborado pelo próprio autor

As três primeiras questões foram direcionadas ao componente atenção, isto é, acerca da atenção que os alunos deram à sequência e como ela conseguiu chamar sua atenção. De acordo com a Figura 21, percebemos que a Questão 01 da pesquisa de avaliação, que indagava se as atividades propostas chamaram a atenção do aluno, mostrou que 60%, o que equivale a 15 alunos, disseram sim, 8% disseram não, equivalente a 2 alunos, e 32%, equivalente a 8 alunos, disseram às vezes.

Figura 21 – Questão 1



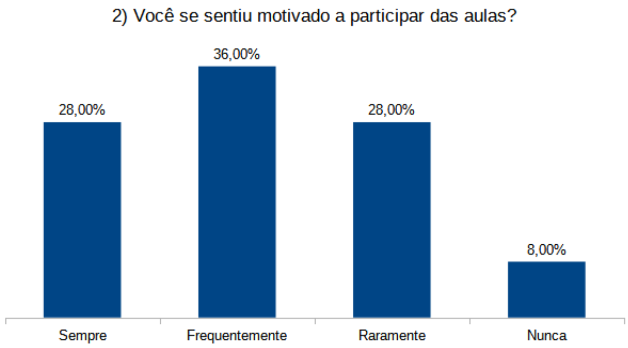
Fonte: Elaborado pelo próprio autor

Observa-se que apenas dois alunos afirmaram que nenhum aspecto da sequência didática chamou sua atenção. Isso indica que 23 dos 25 respondentes demonstraram interesse e envolvimento desde o início da aplicação da proposta.

De acordo com a Figura 22, percebemos que a Questão 02 da pesquisa de avaliação, que indagava se o aluno se sentiu motivado com as atividades propostas, mostrou que 28%, o que equivale a 7 alunos, disseram sempre, 36% disseram frequentemente, equivalente a 9 alunos, 28%, equivalente a 7 alunos, e 8%, equivalente a 2 alunos disseram nunca.

A análise desta questão mostrou que somente dois alunos afirmaram não terem se sentido motivados por nenhum aspecto da sequência didática. Com isso, infere-se que a maioria dos participantes demonstrou motivação para participar da proposta desde o início de sua aplicação.

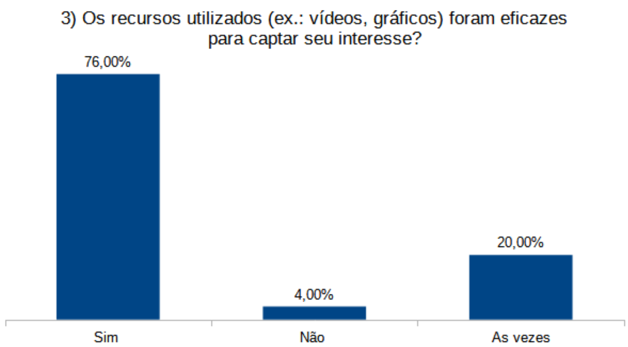
Figura 22 – Questão 2



Fonte: Elaborado pelo próprio autor

De acordo com a Figura 23, percebemos que a Questão 03 da pesquisa de avaliação, que indagava se os recursos utilizados (ex.: vídeos, gráficos) foram eficazes para captar o interesse do aluno, mostrou que 76%, o que equivale a 19 alunos, disseram sim, 4% disseram não, equivalente a 1 aluno, e 20%, equivalente a 5 alunos, disseram às vezes.

Figura 23 – Questão 3



Fonte: Elaborado pelo próprio autor

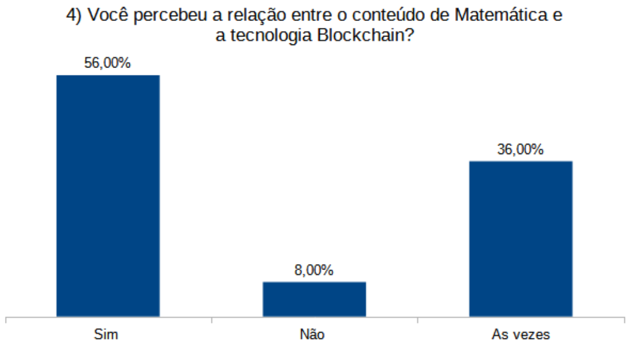
Nessa questão três, apenas um aluno afirmou não ter encontrado, entre os recursos utilizados (como vídeos e gráficos), elementos capazes de despertar seu interesse. Dessa forma, 24 dos 25 respondentes demonstraram interesse e empolgação em participar da sequência didática.

As Questões 01 a 03 investigam o componente atenção, e os resultados indicam que a maioria dos alunos considerou as atividades propostas atraentes e motivadoras. Na Questão 01, 60% dos alunos afirmaram que as atividades chamaram sua atenção, o que pode estar diretamente relacionado à escolha de um tema contemporâneo e pouco usual no ensino de matemática, como o *Bitcoin*. A curiosidade gerada por esse conteúdo, aliado à proposta metodológica, favoreceu a manutenção do interesse dos estudantes ao longo da sequência. A utilização de recursos diferenciados, como vídeos, gráficos e simulações práticas, também contribuiu significativamente, como apontado na questão

03, em que 76% dos alunos indicaram que esses materiais foram eficazes para despertar o interesse.

As Questões 4, 5, e 6 foram relacionadas ao componente relevância, ou seja, o quanto os alunos acharam o conteúdo de sequência, progressões e a tecnologia *blockchain* relevante para seu aprendizado a partir dessa metodologia. Conforme a Figura 24, percebemos que a Questão 04 da pesquisa de avaliação, que questiona se o aluno percebeu a relação entre o conteúdo de Matemática e a tecnologia *blockchain*, mostrou que 56%, o que equivale a 14 alunos, disseram sim, 8% disseram não, equivalente a 2 alunos, e 36%, equivalente a 9 alunos, disseram às vezes.

Figura 24 – Questão 4



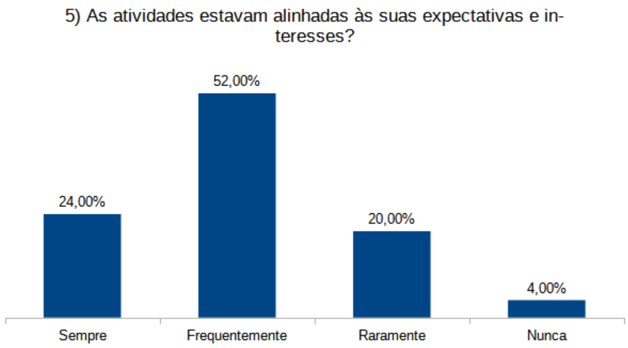
Fonte: Elaborado pelo próprio autor

Nessa Questão 4, apenas 2 afirmaram não perceber a relação entre a matemática e a tecnologia *blockchain* do *Bitcoin*, ou seja, 23 dos 25 alunos que responderam a pergunta conseguiram perceber a relação existente entre os blocos da rede *bitcoin* e o conteúdo de sequências e progressões.

De acordo com a Figura 25, percebemos que a Questão 05 da pesquisa de avaliação, que questiona se as atividades estavam alinhadas às expectativas dos alunos, mostrou que 24%, o que equivale a 6 alunos, disseram sempre, 52% disseram frequentemente, equivalente a 13 alunos, 20%, equivalente a 5 alunos, e 4%, equivalente a 1 aluno que disse nunca.

Nessa Questão 5, apenas 1 afirmou que as atividades propostas na sequência didática não estavam alinhadas às expectativas sobre matemática e tecnologia *blockchain* do *bitcoin*. Ou seja, 24 alunos afirmaram que em algum momento tinham as expectativas alinhadas aos interesses sobre o conteúdo.

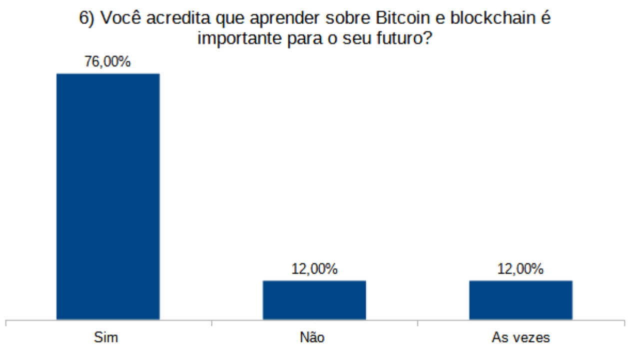
Figura 25 – Questão 5



Fonte: Elaborado pelo próprio autor

Na Figura 26, apresentamos os resultados da Questão 06 da pesquisa, que investiga a percepção dos alunos sobre a relevância de aprender sobre *Bitcoin* e *blockchain* para suas perspectivas futuras. A pesquisa revelou que 76% dos participantes (equivalente a 19 alunos) acreditam que esse conhecimento é importante, enquanto 12% (3 alunos) afirmaram que não consideram relevante. Além disso, 12% dos respondentes (também 3 alunos) indicaram que às vezes enxergam valor nesse aprendizado.

Figura 26 – Questão 6



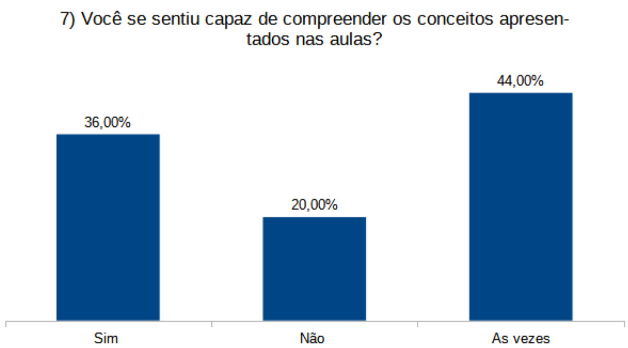
Fonte: Elaborado pelo próprio autor

Nessa Questão 6, dos alunos que reconhecem a importância do aprendizado sobre *Bitcoin* e *blockchain* pode ser interpretada como um reflexo do crescente interesse e influência dessas tecnologias no mercado financeiro e nas inovações digitais. Os três alunos que responderam **não** pode ser resultado de experiências pessoais que não corroboram a importância das tecnologias em suas áreas de interesse.

Nas Questões 04 a 06, relacionadas à dimensão relevância, os dados revelam que a maioria dos estudantes percebeu valor na articulação entre os conteúdos matemáticos e a tecnologia *blockchain*. Na Questão 04, 56% dos alunos reconheceram a relação direta entre o conteúdo de matemática e a estrutura da rede *Bitcoin*. Isso demonstra que a contextualização dos conteúdos em um cenário tecnológico contemporâneo contribuiu para dar sentido ao que estava sendo aprendido. A Questão 05 reforça essa percepção, pois 76% dos alunos relataram que as atividades estavam alinhadas às suas expectativas, indicando que houve conexão entre os interesses dos estudantes e os objetivos da proposta. Já a Questão 06 revelou que 76% dos alunos enxergam importância no aprendizado sobre *Bitcoin* e *Blockchain* para sua vida futura, o que pode ser atribuído ao crescente interesse por temas ligados a finanças digitais e inovação tecnológica. Essa resposta sugere que, ao abordar um conteúdo com relevância social e econômica, a sequência didática fortaleceu o engajamento dos alunos com a matemática escolar.

As Questões de número 7 a 9 foram direcionadas a investigar o componente relacionado à confiança. Em outras palavras, essas perguntas buscavam avaliar o quanto os alunos se sentiram confiantes em relação ao conhecimento e às habilidades adquiridas ao longo da execução da sequência didática. A Figura 27, que ilustra os resultados da Questão 07 da pesquisa, que questiona os alunos sobre sua capacidade de compreender os conceitos abordados durante as aulas. 36% dos participantes (equivalente a 9 alunos) se sentiram capazes de entender os conteúdos apresentados, enquanto 20% (5 alunos) relataram que não conseguiram compreendê-los. Por outro lado, a maior parte dos respondentes, 44% (11 alunos), afirmou que às vezes se sentiu capaz de entender os conceitos

Figura 27 – Questão 7

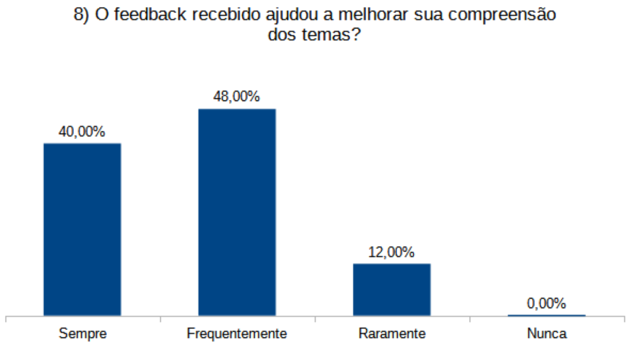


Fonte: Elaborado pelo próprio autor.

Nessa questão sete, os alunos foram questionados sobre sua capacidade de compreender os conceitos ensinados durante as aulas. Nove alunos se sentiram capazes de entender os conceitos pode ser vista como um sinal positivo, indicando que uma parte significativa da turma está assimilando o conteúdo. Contudo, o fato de 5 alunos terem dito não compreender os conceitos sugere que existem desafios que precisam ser abordados para garantir uma melhor assimilação.

Conforme a Figura 28, que apresenta os resultados da Questão 08 da pesquisa, que investiga se o *feedback* recebido pelos alunos contribuiu para melhorar sua compreensão dos temas discutidos. Os dados mostram que 40% dos participantes (equivalente a 10 alunos) afirmaram que o suporte ajudou sempre na compreensão dos conteúdos. Além disso, 48% (12 alunos) indicaram que o retorno foi útil frequentemente. Por outro lado, 12% (3 alunos) relataram que o *feedback* ajudou raramente ou nunca.

Figura 28 – Questão 8

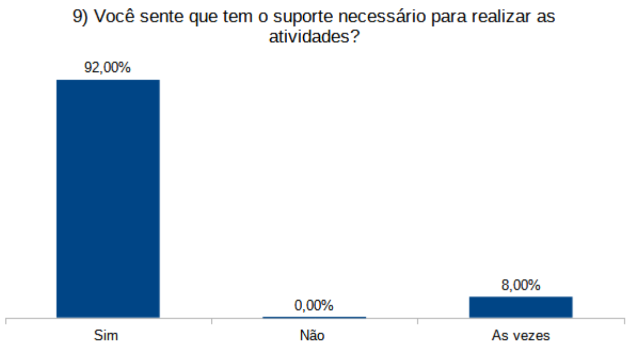


Fonte: Elaborado pelo próprio autor

Ao questionar os alunos sobre o *feedback* recebido se teria contribuído para a compreensão dos temas discutidos, nessa Questão 8, 10 alunos afirmaram que o retorno as perguntas sempre os ajudou, e 12 alunos disseram frequentemente. Esse resultado é positivo, pois indica que a maioria reconheceu o valor do suporte no processo de aprendizagem. No entanto, os 3 alunos que relataram raramente sugerem que ainda há espaço para aprimorar a forma como o *feedback* é oferecido.

Conforme a Figura 29, que apresenta os resultados da Questão 09 da pesquisa, que avalia se os alunos sentem que possuem o suporte necessário para realizar as atividades. A pesquisa revelou que 92% dos participantes (equivalente a 23 alunos) afirmaram que se sentem apoiados, enquanto apenas 8% (2 alunos) indicaram que às vezes possuem esse suporte. Nenhum aluno mencionou que não recebeu suporte.

Figura 29 – Questão 9



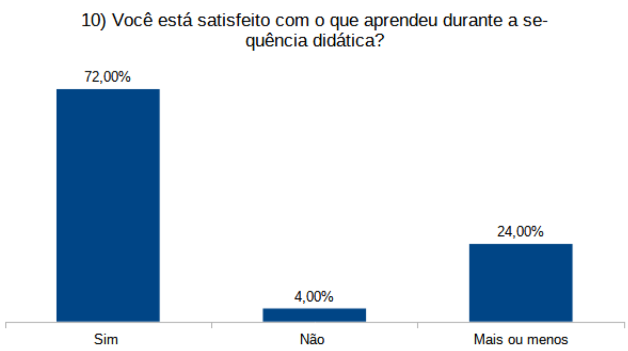
Fonte: Elaborado pelo próprio autor

Nessa Questão 09, investigou-se se os alunos sentem que possuem o suporte necessário para realizar as atividades. Dos 25 alunos, 23 afirmaram que se sentem apoiados, o que indica um resultado bastante positivo para o processo de ensino. Apenas 2 alunos disseram que recebem esse suporte às vezes, o que sugere a necessidade de atenção pontual para garantir que todos se sintam plenamente assistidos.

O componente confiança foi avaliado pelas Questões 07 a 09. A Questão 07 evidenciou que embora 36% dos alunos tenham se sentido plenamente capazes de compreender os conceitos abordados, uma parcela expressiva (44%) afirmou que às vezes conseguiu acompanhar, o que sinaliza a necessidade de atenção ao ritmo e às estratégias de explicação utilizadas. Ainda assim, os dados demonstram que a maioria sentiu-se envolvida cognitivamente e foi capaz de avançar com apoio. A Questão 08 reforça esse ponto, pois 88% dos alunos consideraram o *feedback* recebido como útil para melhorar sua compreensão. Esse dado é extremamente positivo, pois destaca o papel do professor como mediador da aprendizagem, capaz de oferecer devolutivas significativas durante a realização das atividades. Na Questão 09, a percepção de suporte também se mostrou elevada: 92% dos estudantes afirmaram sentir que receberam o apoio necessário para realizar as tarefas, evidenciando um ambiente de aprendizagem acolhedor, estruturado e colaborativo.

Por fim, as Questões de 10 a 12 tiveram como foco o componente satisfação. Essas perguntas procuraram avaliar o nível de contentamento dos alunos em relação à participação na sequência didática, considerando tanto a percepção sobre o aprendizado alcançado e o quanto essa experiência contribuiu para aumentar sua motivação para estudar os conteúdos abordados. A Figura 30, apresenta os resultados da Questão 10 da pesquisa, que investiga se os alunos estão satisfeitos com o que aprenderam durante a sequência didática. A pesquisa revelou que 72% dos participantes (equivalente a 18 alunos) expressaram satisfação, enquanto 4% (1 aluno) informaram que não estão satisfeitos. Além disso, 24% (6 alunos) indicaram que estão mais ou menos satisfeitos.

Figura 30 – Questão 10

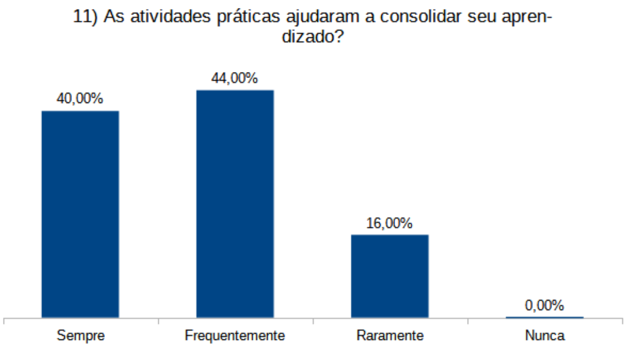


Fonte: Elaborado pelo próprio autor

Nessa Questão 10, dezoito afirmaram estar satisfeitos com os conhecimentos adquiridos, o que demonstra que a maioria percebeu ganhos concretos no processo de aprendizagem. Outros 6 alunos relataram estar apenas parcialmente satisfeitos, o que pode indicar dúvidas pontuais ou expectativa de aprofundamento. Apenas 1 aluno declarou não estar satisfeito, apontando a importância de investigar possíveis dificuldades ou falta de conexão com a metodologia para garantir que todos sejam contemplados.

A Figura 31, ilustra os resultados da Questão 11 da pesquisa, que avalia se as atividades práticas ajudaram os alunos a consolidar seu aprendizado. A pesquisa revelou que 40% dos participantes (equivalente a 10 alunos) afirmaram que as atividades ajudaram sempre na consolidação do aprendizado. Além disso, 44% (11 alunos) relataram que as atividades foram úteis frequentemente. Por outro lado, 16% (4 alunos) indicaram que as atividades ajudaram raramente.

Figura 31 – Questão 11



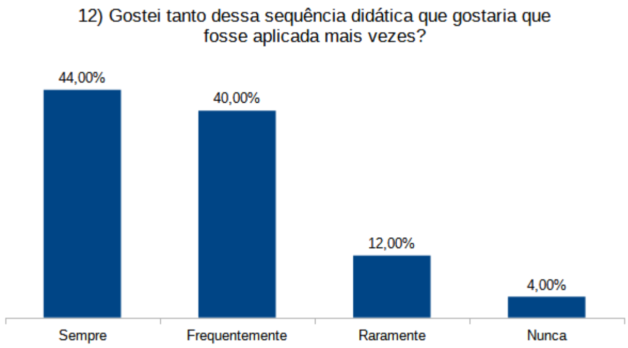
Fonte: Elaborado pelo próprio autor

Na Questão 11, dez afirmaram que essas atividades sempre ajudaram, enquanto 11 relataram que foram úteis com frequência. Esses dados indicam que a maioria reconheceu as atividades práticas como elemento importante para a aprendizagem. No entanto, 4 alunos disseram que as atividades ajudaram raramente, o que sugere a necessidade de repensar a aplicação ou o nível de acessibilidade dessas práticas para melhor atender a todos.

Finalmente a Figura 32, apresenta os resultados da Questão 12 da pesquisa, que investiga o grau de satisfação dos alunos em relação à sequência didática e seu desejo de que ela fosse aplicada mais vezes. A pesquisa revelou que 44% dos participantes (equivalente a 11 alunos) expressaram que gostariam que a sequência fosse aplicada sempre. Além disso, 40% (10 alunos) indicaram que gostariam disso frequentemente. Apenas 4% (1 aluno) afirmaram que gostariam que a sequência fosse aplicada raramente ou nunca.

Esses dados da Questão 12 indicam que a maioria dos alunos reconheceu valor pedagógico e relevância na proposta, o que reforça a efetividade de integrar temas tecnológicos, como a rede *Bitcoin*, ao ensino da matemática. O pequeno percentual que respondeu nunca pode estar relacionado a preferências individuais ou à familia-

Figura 32 – Questão 12



Fonte: Elaborado pelo próprio autor

ridade prévia com o tema, mas não compromete a evidência de aceitação positiva da metodologia.

Na avaliaram do componente satisfação. A maioria dos alunos (72%) declarou-se satisfeita com o que aprenderam durante a sequência, conforme os dados da Questão 10, o que demonstra que a metodologia utilizada alcançou seus objetivos pedagógicos. Essa satisfação também pode estar associada à percepção de utilidade do conteúdo, à possibilidade de participar de atividades práticas e ao ambiente favorável ao diálogo. A Questão 11 revelou que 84% dos alunos consideraram que as atividades práticas contribuíram para consolidar o aprendizado, reforçando a importância de abordagens que aliam teoria e prática no ensino da matemática. Por fim, a Questão 12 destacou que 84% dos participantes gostariam que a sequência didática fosse aplicada com mais frequência, o que evidencia não apenas a aprovação da proposta, mas também o desejo dos alunos por experiências de aprendizagem significativas, inovadoras e conectadas ao mundo contemporâneo.

Observamos que, de forma geral, a maioria dos alunos respondeu de maneira favorável às questões de cada um dos componentes avaliados pelo modelo ARCS. Ainda destacamos que nas questões relacionadas à atenção e relevância, grande parte dos estudantes afirmou ter percebido uma conexão significativa entre os conteúdos matemáticos e a aplicação prática com a tecnologia *blockchain*, o que demonstra que a metodologia utilizada conseguiu despertar o interesse e a percepção de utilidade do tema abordado. Quanto ao componente confiança, as respostas indicam que os alunos se sentiram capazes de compreender os conceitos apresentados e realizar as atividades propostas, mostrando que a sequência foi planejada de maneira acessível e desafiadora na medida certa.

Por fim, no que se refere à satisfação, o número expressivo de alunos que se mostrou satisfeito com o que aprenderam, além de declararem o desejo de vivenciar novamente esse tipo de proposta, reforça o impacto positivo da abordagem adotada. A aplicação do modelo ARCS nesta avaliação proporcionou uma visão ampla e estruturada sobre o impacto motivacional da sequência didática. Considerando os aspectos do modelo ARCS, é possível afirmar que a metodologia utilizada favoreceu não apenas o engajamento dos alunos, mas também contribuiu de forma efetiva para o processo de ensino e aprendizagem de conteúdos matemáticos de forma contextualizada e significativa.

6 Considerações Finais

Nesta dissertação apresentamos uma proposta para o ensino da Matemática no Ensino Médio, ao integrar conceitos fundamentais de sequências e progressões com a tecnologia da rede do *Bitcoin*. Essa abordagem contribui para tornar a matemática mais concreta, prática e atraente para os estudantes, ao conectá-la a um tema atual e de grande impacto social e tecnológico.

Esse trabalho destaca que a utilização da rede do *Bitcoin* como ferramenta didática permite que os alunos compreendam não apenas os aspectos teóricos das sequências numéricas, PA e PG, mas também sua aplicação direta em um contexto real e tecnológico. Essa conexão entre teoria e prática favorece o desenvolvimento do pensamento lógico, crítico e a capacidade de resolução de problemas, competências essenciais para a formação integral dos estudantes.

Além disso, essa dissertação enfatiza a importância da BNCC como referência para o desenvolvimento das competências gerais e específicas, especialmente no que tange à valorização do conhecimento histórico, cultural e digital, bem como ao uso crítico e ético das tecnologias digitais. A proposta pedagógica apresentada está alinhada a essas diretrizes, promovendo uma aprendizagem significativa e contextualizada.

A proposta mostra-se relevante diante do desafio constante enfrentado por professores: captar e manter a atenção dos estudantes em um cenário onde as tecnologias digitais, redes sociais, aplicativos e jogos, exercem forte influência sobre a rotina dos jovens. Nesse contexto, a utilização dessa metodologia, associação de blocos da rede *Bitcoin*, aliada ao uso de contextos reais, desponta como um caminho promissor no processo de ensino-aprendizagem.

A aplicação da sequência didática mostrou resultados positivos, aumentando o engajamento, a cooperação e o desempenho dos alunos. Eles participaram mais ativamente, demonstraram interesse e desenvolveram habilidades matemáticas mais críticas. O questionário baseado no modelo ARCS confirmou que a metodologia despertou atenção, relevância, confiança e satisfação, essenciais para a aprendizagem significativa.

Concluímos, portanto, que a incorporação de temas do mundo digital e o uso de metodologias motivacionais, como a associação de blocos da rede *Bitcoin*, podem contribuir significativamente para tornar a matemática mais atrativa, compreensível e conectada à realidade dos estudantes. Espera-se que este trabalho inspire novos estudos, adaptações e experimentações que fortaleçam o vínculo entre matemática, tecnologia e ensino significativo.

Referências

BALESTRA, M. M. M. *A psicopedagogia em Piaget: uma ponte para a educação da liberdade*. [S.l.]: Ibpex, 2007. Citado na página 19.

BRASIL. *Base Nacional Comum Curricular*. 2017. Disponível em: <https://www.gov.br/mec/pt-br/escola-em-tempo-integral/BNCC_EI_EF_110518_versaofinal.pdf>. Acesso em: 20 jan. 2025. Citado 4 vezes nas páginas 16, 17, 18 e 51.

CARVALHO, P. C. P.; MORGADO, A. C. *Matemática Discreta*. [S.l.]: Sociedade Brasileira de Matemática (SBM), 2017. Coleção PROFMAT. Citado 2 vezes nas páginas 24 e 50.

CORREA, L. A.; TANIGUTI, G.; FERREIRA, K. *Tecnologias Digitais Aplicadas à Educação Inclusiva: Fortalecendo o Desenho Universal para a Aprendizagem*. Instituto Rodrigo Mendes, 2021. ISBN 978-65-5854-467-8. Disponível em: <https://institutorodrigomendes.org.br/wp-content/uploads/2021/11/Tecnologias-digitais-aplicadas-a-educacao-inclusiva-IRM.pdf>. Citado 2 vezes nas páginas 17 e 50.

COUTINHO, C. *Criptografia*. [S.l.]: Editora, 2015. Citado na página 40.

GONZAGA, R. do N. *Bitcoin: uma introdução à matemática das transações*. Dissertação (Mestrado) — Pontifícia Universidade Católica do Rio de Janeiro, Rio de Janeiro, 2021. Dissertação de Mestrado, Departamento de Matemática, PUC-Rio. Orientador: Sinésio Pesco. Citado na página 22.

LEãO, L. C. da S. *Uma introdução ao estudo de bitcoins e blockchains*. Dissertação (Mestrado) — Universidade Federal do Estado do Rio de Janeiro, Rio de Janeiro, 2019. Dissertação de Mestrado, Programa de Pós-Graduação em Matemática, UNIRIO. Orientador: Silas Fantin. Citado na página 22.

LIMA, E. L. *Conceituação, Manipulação e Aplicações Os Três Componentes do Ensino da Matemática*. 1999. Disponível em: <https://www.ufrgs.br/espmat/disciplinas/midias_digitais_II/modulo_II/pdf/rpm41.pdf>. Acesso em: 30 ago 2024. Citado na página 18.

MARQUES, C. P. *A importância da Análise Real na formação do Professor de Matemática do Ensino Médio: o caso das sequências numéricas*. Dissertação (Dissertação (Mestrado)) — PROFMAT, Universidade Federal de Campina Grande (UFCG), 2019. Citado 5 vezes nas páginas 20, 24, 25, 50 e 51.

NAKAMOTO, S. *Bitcoin: um sistema de dinheiro eletrônico peer-to-peer*. 2008. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 30 ago 2024. Citado 3 vezes nas páginas 13, 33 e 50.

PARAíBA. *PCEMPB*. 2021. Secretaria de Educação do Estado da Paraíba. Citado 2 vezes nas páginas 20 e 49.

RAMOS, M. R. V. O uso de tecnologias em sala de aula. *2 Edição Nº. 2, Vol. 1*, UEL, p. 1–15, 2012. Disponível em: <https://www.uel.br/revistas/lenpes-pibid/pages/arquivos/2%20Edicao/MARCIO%20RAMOS%20-%20ORIENT%20PROF%20ANGELA.pdf>. Citado 2 vezes nas páginas 19 e 20.

RODRIGUES, A. M. *O uso da Novas tecnologias na educação*. 121 p. Dissertação (Monografia (Especialização em Fundamentos da Educação: Práticas Pedagógicas Interdisciplinares)) — Universidade Estadual da Paraíba, 2014. Citado na página 21.

SIGLER, L. *Fibonacci's Liber Abaci*. [S.l.]: Springer, 2002. Citado na página 25.

ULRICH, F. *BITCOIN - A MOEDA NA ERA DIGITAL*. [S.l.]: Instituto Ludwig Von Mises Brasil, 2014. Citado 5 vezes nas páginas 13, 33, 40, 47 e 50.

ZABALA, A. *A prática educativa : como ensinar [recurso eletrônico]*. [S.l.]: Editora ABDR, 1998. Citado 2 vezes nas páginas 19 e 49.

Apêndices

APÊNDICE A – Questionário sobre a avaliação metodológica da sequência didática

Pesquisa de Avaliação

Este questionário tem como objetivo obter as opiniões dos alunos participantes da sequência didática **cadeia de blocos da rede Bitcoin no ensino de Sequências e Progressões**, realizada nas aulas de Matemática pelo professor Emerson Rodrigues Alves, utilizando o modelo ARCS (Atenção, Relevância, Confiança e Satisfação).

Aluno(a): ____

Parte 1: Atenção

1. As atividades propostas chamaram sua atenção?
   ( ) Sim ( ) Não ( ) Às vezes

2. Você se sentiu motivado a participar das aulas?
   ( ) Sempre ( ) Frequentemente ( ) Raramente ( ) Nunca

3. Os recursos utilizados (ex.: vídeos, gráficos) foram eficazes para captar seu interesse?
   ( ) Sim ( ) Não ( ) Às vezes

Parte 2: Relevância

4. Você percebeu a relação entre o conteúdo de Matemática e a tecnologia Blockchain?
   ( ) Sim ( ) Não ( ) Às vezes

5. As atividades estavam alinhadas às suas expectativas e interesses?
   ( ) Sempre ( ) Frequentemente ( ) Raramente ( ) Nunca

6. Você acredita que aprender sobre Bitcoin e blockchain é importante para o seu futuro?
   ( ) Sim ( ) Não ( ) Às vezes

Parte 3: Confiança

7. Você se sentiu capaz de compreender os conceitos apresentados nas aulas?
( ) Sim ( ) Não ( ) Às vezes

8. O feedback recebido ajudou a melhorar sua compreensão dos temas?
( ) Sempre ( ) Frequentemente ( ) Raramente ( ) Nunca

9. Você sente que tem o suporte necessário para realizar as atividades?
( ) Sim ( ) Não ( ) Às vezes

Parte 4: Satisfação

10. Você está satisfeito com o que aprendeu durante a sequência didática?
( ) Sim ( ) Não ( ) Às vezes

11. As atividades práticas ajudaram a consolidar seu aprendizado?
( ) Sempre ( ) Frequentemente ( ) Raramente ( ) Nunca

12. Gostei tanto dessa sequência didática que gostaria que fosse aplicada mais vezes?
( ) Sempre ( ) Frequentemente ( ) Raramente ( ) Nunca

APÊNDICE B – Recurso Educacional

UNIVERSIDADE FEDERAL DE CAMPINA GRANDE
Programa de Pós-Graduação em Matemática
Mestrado Profissional - PROFMAT/CCT/UFCG

Émerson Rodrigues Alves

Recurso Educacional

Uma proposta didática sobre sequências e progressões com a cadeia de blocos do Bitcoin

Campina Grande - PB
Agosto/2025

UNIVERSIDADE FEDERAL DE CAMPINA GRANDE
Programa de Pós-Graduação em Matemática
Mestrado Profissional - PROFMAT/CCT/UFCG

Émerson Rodrigues Alves

Uma proposta didática sobre sequências e progressões com a cadeia de blocos do Bitcoin

Recurso Educacional vinculado ao Trabalho de Conclusão de Curso apresentado ao Corpo Docente do Programa de Pós-Graduação em Matemática - CCT - UFCG, na modalidade Mestrado Profissional, como requisito parcial para obtenção do título de Mestre.

Orientador: Dr(a). Deise Mara Barbosa de Almeida
Coorientador: Dr. Leomaques Francisco Silva Bernardo

Campina Grande - PB
Agosto/2025

Resumo

A matemática é uma disciplina fundamental para o desenvolvimento do pensamento lógico, da capacidade de resolver problemas e da compreensão das relações numéricas que permeiam nosso cotidiano e a evolução tecnológica da sociedade. Este trabalho apresenta uma proposta de sequência didática voltada ao ensino de sequências numéricas e progressões aritméticas e geométricas, integrando conceitos da tecnologia *Blockchain* e da rede Bitcoin. A ideia central é utilizar a estrutura da cadeia de blocos do *Bitcoin* como contexto prático para motivar os alunos e unir o conteúdo matemático com tecnologia com objetivo de desenvolver a compreensão dos alunos sobre sequências numéricas, incluindo sequências aritméticas e geométricas. A proposta pode ser aplicada em turmas do Ensino Médio ou Ensino Fundamental. Propõe-se uma abordagem de aprendizagem ativa, fundamentada na articulação entre os conceitos matemáticos e o uso da tecnologia como recurso didático.

Palavras-chave: Sequências; Progressões; Sequências Didáticas; Bitcoin; Blockchain.

Abstract

Mathematics is a fundamental discipline for the development of logical thinking, problem-solving skills, and the understanding of numerical relationships that permeate our daily lives and the technological advancement of society. This work presents a didactic sequence proposal focused on the teaching of numerical sequences and arithmetic and geometric progressions, integrating concepts from Blockchain technology and the Bitcoin network. The central idea is to use the structure of Bitcoin's blockchain as a practical context to motivate students and to connect mathematical content with technology, aiming to enhance students' understanding of numerical sequences, including arithmetic and geometric sequences. The proposal can be applied in both high school and middle school settings. The methodology adopted seeks to promote active learning through the articulation between mathematics and technology.

Keywords: Progressions; Didactic Sequences; Bitcoin; Blockchain.

1 Introdução

A matemática, por vezes percebida como abstrata e distante da realidade cotidiana, pode assumir um papel transformador quando integrada a contextos significativos para os estudantes. A presente proposta de produto educacional visa suprir essa lacuna ao integrar o ensino de sequências e progressões com o universo de tecnologia, mais especificamente com a rede do Bitcoin e sua estrutura em cadeia de blocos (blockchain).

As sequências e progressões, pertencentes à unidade temática de Álgebra na Base Nacional Comum Curricular (BNCC), constituem-se em ferramentas essenciais para a organização e a compreensão de padrões numéricos. Uma sequência é uma lista ordenada de números, sendo cada elemento denominado termo. Entre as diversas classificações possíveis, destacam-se as progressões aritméticas (PA), nas quais há uma diferença constante entre termos consecutivos, e as progressões geométricas (PG), que apresentam uma razão constante entre os termos.

Este trabalho tem como objetivo integrar o ensino desses conceitos a uma aplicação concreta e atual: a cadeia de blocos do Bitcoin. O Bitcoin, conforme Nakamoto (2008), criador do protocolo, descreve a blockchain como uma estrutura de dados descentralizada que registra de maneira pública e imutável todas as transações realizadas na rede Bitcoin.

A blockchain é composta por uma sequência encadeada de blocos, cada um contendo informações como um conjunto de transações, a marca temporal (timestamp), o hash do bloco anterior e o nonce — elemento usado no processo de mineração. Antes de serem inseridas na cadeia, as transações são temporariamente armazenadas na mempool, onde aguardam validação. Esse funcionamento pode ser interpretado matematicamente como uma sequência, cuja organização linear garante a integridade e segurança das informações.

A estrutura sequencial da blockchain oferece um cenário ideal para a exploração de sequências numéricas e progressões em sala de aula. Com base nisso, foi elaborada uma sequência didática composta por sete encontros. Durante as aulas, os alunos podem trabalhar com a sequência de Fibonacci, progressões aritméticas e geométricas, contextualizando tais conceitos através da rede Bitcoin e utilizando ferramentas digitais como o site mempool.space para visualização dos blocos em tempo real.

A proposta metodológica deste trabalho envolve aulas expositivas, resolução de problemas, atividades práticas e avaliação formativa. O objetivo principal é desenvolver o raciocínio lógico e a capacidade dos estudantes de aplicar os conceitos matemáticos em contextos reais e tecnológicos. Acredita-se que, ao aproximar os conteúdos escolares de temas atuais e relevantes, como a tecnologia da rede do Bitcoin, seja possível tornar o aprendizado mais significativo, contribuindo para a melhoria do desempenho acadêmico e para a formação dos alunos.

1.1 Objetivos

1.1.0.1 Objetivo Geral

Desenvolver a compreensão dos alunos sobre sequências numéricas, incluindo sequências aritméticas e geométricas, e sua relevância na matemática e na tecnologia.

1.1.0.2 Objetivos Específicos

- Identificar e classificar diferentes tipos de sequências numéricas (finita, infinita, recorrente, não recorrente);
- Introduzir os conceitos básicos da rede Bitcoin e sua importância;
- Explicar a estrutura de blockchain e como a mempool armazena transações em sequência;
- Relacionar a estrutura da blockchain com sequências numéricas e progressões;
- Ensinar a classificar progressões aritméticas e identificar suas características;
- Determinar o termo geral de uma PA e aplicá-lo na análise de recompensas em Bitcoin;
- Promover a resolução de problemas práticos que envolvam PA, especialmente em cenários de mineração;
- Introduzir a classificação e o termo geral das progressões geométricas;
- Relacionar PG às recompensas de Bitcoin a cada bloco minerado, demonstrando a aplicação matemática;
- Discutir o conceito do limite total de Bitcoin que pode ser minerado, conectando matemática e tecnologia.

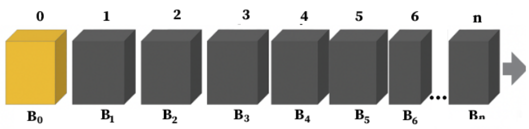
1.2 Organização

Visando o cumprimento dos objetivos estabelecidos na Seção 1.1, este produto educacional está estruturado em quatro capítulos. O Capítulo 1 apresenta os aspectos introdutórios, bem como a definição dos objetivos deste trabalho. No Capítulo 2, realiza-se uma descrição sucinta da rede *Bitcoin*, abordando seus principais conceitos e características. O Capítulo 3 dedica-se à exposição detalhada da sequência didática, incluindo os procedimentos para sua aplicação. Por fim, o Capítulo 4 traz as considerações finais acerca da sequência didática desenvolvida, destacando os resultados alcançados e possíveis desdobramentos futuros.

2 Rede Bitcoin

Neste capítulo, faremos uma breve apresentação da rede *Bitcoin*, com o objetivo de facilitar a compreensão dos conceitos e tornar a leitura da sequência didática mais acessível. A rede *Bitcoin*, criada por Nakamoto (2008), é uma estrutura descentralizada que permite a realização de transações digitais seguras e verificáveis sem a necessidade de uma autoridade central. Seu funcionamento baseia-se em uma tecnologia chamada *blockchain*, ou cadeia de blocos, na qual cada bloco contém um conjunto de transações, a referência ao bloco anterior por meio de um código chamado *hash* e outros dados técnicos. Essa estrutura forma uma sequência ordenada, encadeada e cronológica de blocos — uma característica que estabelece um vínculo direto com os conceitos matemáticos de sequência e progressão, como a Figura 1.

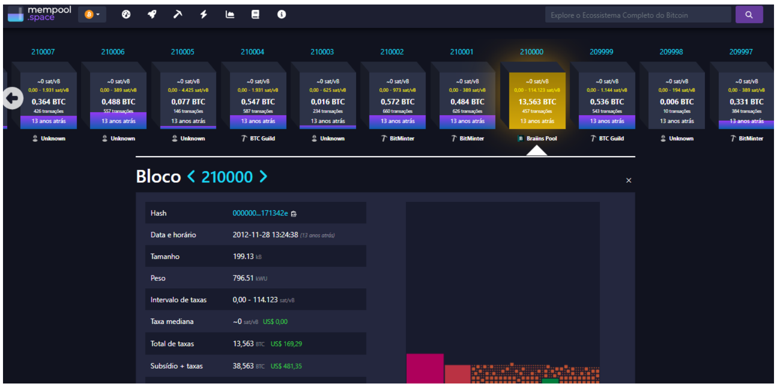
Figura 1 – Blockchain



Fonte: Elaborado pelo autor (2025)

No contexto educacional, essa organização sequencial da *blockchain* pode ser utilizada como recurso pedagógico para explorar e exemplificar diversos tópicos do componente curricular de Matemática, especialmente as sequências numéricas, as progressões aritméticas (PA) e as progressões geométricas (PG). A cada novo bloco adicionado à rede, há um número crescente e único associado, o que configura uma progressão aritmética de razão 1. Além disso, a política monetária do *Bitcoin* determina que a recompensa por bloco minerado seja reduzida pela metade a cada 210 mil blocos — um processo conhecido como *halving* — e que forma uma progressão geométrica decrescente. Na Figura 2, observa-se o bloco de número 210.000, no qual foram minerados 25 BTC como recompensa base, além de 13,563 BTC provenientes das taxas de transação. Antes desse marco, a recompensa por bloco era de 50 BTC, mas, a partir desse ponto, ocorreu o primeiro *halving*, reduzindo a recompensa para 25 BTC conforme previsto no protocolo do *Bitcoin*.

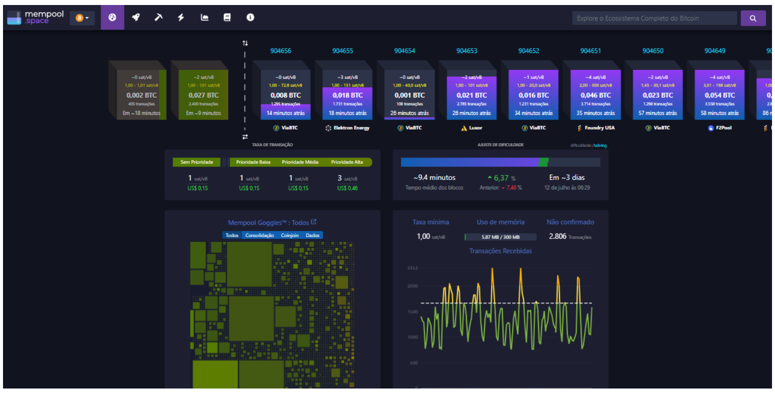
Figura 2 – Bloco 210 mil



Fonte: Elaborado pelo autor (2025)

Para ilustrar essas relações em sala de aula, pode-se utilizar o site <https://mempool.space/pt>, uma plataforma que permite a visualização em tempo real dos blocos sendo minerados na rede, Figura 3. A partir da análise visual dessa cadeia, os alunos podem identificar a sequência cronológica de blocos e as transações contidas em cada um, percebendo padrões e regularidades que refletem diretamente os conceitos matemáticos estudados. O recurso digital torna o conteúdo mais acessível e concreto, promovendo o engajamento e facilitando a compreensão de temas tradicionalmente abstratos.

Figura 3 – mempool



Fonte: Elaborado pelo autor (2025)

Essa abordagem permite que o professor integre, de forma significativa, a matemática escolar ao universo tecnológico e contemporâneo, possibilitando não apenas o ensino das propriedades das sequências, mas também sua aplicação em problemas contextualizados. Dessa forma, os alunos desenvolvem habilidades analíticas, pensamento lógico e capacidade de abstração, ao mesmo tempo em que compreendem o funcionamento de uma das tecnologias mais relevantes da atualidade.

No Quadro 1 apresentamos os principais termos técnicos abordados neste documento, com o objetivo de facilitar a compreensão do leitor.

Quadro 1 – Principais termos técnicos sobre

Termos técnicos da rede Bitcoin	
Termo Técnico	**Descrição**
Criptografia	Técnica matemática que protege as transações, garantindo segurança e privacidade.
Chave privada	Código secreto que permite movimentar os bitcoins de uma carteira.
Chave pública	Código visível a todos, usado para receber bitcoins.
Assinatura digital	Prova criptográfica que autentica uma transação, garantindo que foi feita pelo dono da chave privada.
Proof of Work (Prova de Trabalho)	Mecanismo que exige esforço computacional dos mineradores para validar blocos.
Hash	Código alfanumérico gerado por uma função matemática, usado para identificar blocos e transações.
Blockchain	Registro público e imutável de todas as transações realizadas na rede Bitcoin.
Bloco gênese	Primeiro bloco da rede Bitcoin, minerado por Satoshi Nakamoto em 2009.
Bloco	Conjunto de transações agrupadas e registradas na blockchain.
Mempool	Área temporária da rede onde ficam as transações que aguardam confirmação.
Minerador	Participante que usa poder computacional para validar blocos e receber recompensas.
Halving	Evento que reduz pela metade a recompensa por bloco a cada 210.000 blocos minerados.
Recompensa por bloco	Quantidade de bitcoins recebida pelo minerador que valida um bloco.
Taxas de transação	Valor pago pelos usuários para priorizar a inclusão de suas transações em um bloco.
Confirmações de transação	Número de blocos adicionados à blockchain após o bloco que contém uma transação.
Transação	Transferência de bitcoin de um endereço de carteira para outro.
Carteira de bitcoin	softwares que podem criar endereços públicos e privados de bitcoin, visualizar e movimentar saldos.

Fonte: Elaborado pelo próprio autor.

3 Proposta de Sequência Didática

A sequência didática apresentada neste trabalho foi elaborada com o objetivo de promover a aprendizagem significativa de conteúdos matemáticos fundamentais — notadamente, sequências numéricas, progressões aritméticas e progressões geométricas — por meio da articulação com a tecnologia *blockchain*, com foco na rede do *Bitcoin*. A proposta parte da premissa de que a contextualização dos conteúdos matemáticos em situações reais, contemporâneos e tecnologicamente relevantes pode contribuir para o desenvolvimento do pensamento lógico, da autonomia intelectual e do engajamento dos estudantes no processo de aprendizagem.

Ancorada nas diretrizes da Base Nacional Comum Curricular (BNCC) para o Ensino Médio, esta sequência didática foi planejada para ser aplicada em turmas do 1º ano, com carga horária total de 11 horas-aulas. Cada aula foi organizada com base em três eixos estruturais: tempo estimado, desenvolvimento (dividido em dois momentos pedagógicos) e resultados esperados qualitativos, o que favorece a clareza didática e a replicabilidade da proposta por outros docentes.

A metodologia adotada prioriza a resolução de problemas, a mediação ativa do professor e o uso de recursos digitais, como o site mempool.space, que permite a visualização em tempo real da cadeia de blocos da rede *Bitcoin*. As atividades foram estruturadas de forma progressiva, iniciando-se com o conceito de sequência numérica, passando pela análise da sequência de Fibonacci, pela construção e classificação de progressões aritméticas e geométricas, até o estudo de somas de termos e séries infinitas.

A escolha da tecnologia da rede *Bitcoin* como eixo temático não se deu apenas por sua atualidade e relevância, mas principalmente por sua estrutura matemática subjacente, que se mostra adequada à exploração dos conteúdos previstos no componente curricular de Matemática. A sequência de blocos da *blockchain*, a regularidade da emissão de recompensas e o limite teórico da quantidade de *bitcoins* mineráveis foram utilizados como contextos para aplicação dos conceitos de progressão e soma de termos.

Propomos que esta Sequência Didática seja aplicada logo após o estudo de sequência, progressão aritmética e progressão geométrica, sendo necessário toda a assimilação dos conteúdos, bem como a compreensão do funcionamento da rede *Bitcoin*. Sugerimos que, nas primeiras aulas desta Sequência Didática, seja promovido aos alunos uma breve revisão de seguência utilizando o termo lista proposta por (MARQUES, 2019) e uma discussão sobre o que é o *bitcoin*. E nas aulas subsequentes apresentar problemas matemáticos relacionados a rede *Bitcoin*, dos quais irão aumentando o nível de dificuldade de compreensão.

Segundo Zabala (1998), a sequência didática consiste em um conjunto de atividades ordenadas, estruturadas e articuladas que formam uma unidade coerente para alcançar objetivos educacionais específicos. Desse modo, tomaremos como referência as sequências didáticas propostas por Macedo (2023) e Souza (2023), as quais adaptamos para contemplar o conteúdo específico deste trabalho, fundamentando-se na Proposta Curricular do Ensino Médio da Paraíba. Assim, desenvolvemos essa sequência didática para abordar cada um dos conteúdos matemáticos selecionados e sua associação com a rede *Bitcoin*, com 6 aulas, onde cada uma das aulas é organizada por três tópicos: Tempo estimado, Desenvolvimento e Resultados esperados qualitativos, conforme o Quadro 2.

Quadro 2 – Organização das Aulas

Organização dos Encontros	
Aula	**Conteúdo/Atividades**
Aula 01	Introdução à sequências numéricas, elementos de uma sequência, recorrência e termo geral.
Aula 02	Introdução à rede Bitcoin, mempool do Bitcoin e como ela é formada por uma sequência de blocos e transações.
Aula 03	Progressão Aritmética, classificação da PA, termo geral da PA e PA na rede Bitcoin.
Aula 04	Soma da Progressão Aritmética.
Aula 05	Progressão Geométrica, classificação, termo geral da PG. Recompensas em BTC a cada bloco formam uma PG.
Aula 06	Soma dos termos de uma PG finita, soma dos termos de uma PG infinita, soma de unidades de BTC por ciclos; limite total de BTC possível de ser minerado.

Fonte: Elaborado pelo próprio autor.

3.1 Designação da Sequência Didática

Título: Uma sequência didática sobre sequências e progressões com a cadeia de blocos do *Bitcoin*.

Turmas: 1º Ano do Ensino Médio.
Duração: 11 horas-aulas.

Área do conhecimento: Matemática e suas Tecnologias.
Componente curricular: Matemática.

Campo/Eixo: Álgebra e Funções.
Objeto de Conhecimento: Sequências numéricas, Progressão Aritmética e Progressão Geométrica.

Habilidades BNCC:

- (EM13MAT315) Reconhecer um problema algorítmico, enunciá-lo, procurar uma solução e expressá-la por meio de um algoritmo, com o respectivo fluxograma.
- (EM13MAT507) Identificar e associar sequências numéricas (PA) a funções afins de domínios discretos para análise de propriedades, incluindo dedução de algumas fórmulas e resolução de problemas.
- (EM13MAT508) Identificar e associar sequências numéricas (PG) a funções exponenciais de domínios discretos para análise de propriedades, incluindo dedução de algumas fórmulas e resolução de problemas.
- (EM13MAT301) Resolver e elaborar problemas do cotidiano, da Matemática e de outras áreas do conhecimento, que envolvem equações lineares simultâneas, usando técnicas algébricas e gráficas, com ou sem apoio de tecnologias digitais.
- (EM13MAT405) Utilizar conceitos iniciais de uma linguagem de programação na implementação de algoritmos escritos em linguagem corrente e/ou matemática.
- (EF09CO05) - Analisar técnicas de criptografia para armazenamento e transmissão de dados.

Objetivos:

- Identificar e classificar diferentes tipos de sequências numéricas (finita, infinita, recorrente, não recorrente);
- Compreender e exemplificar a sequência de Fibonacci e sua aplicação em contextos práticos;
- Introduzir os conceitos básicos da rede Bitcoin e sua importância;
- Explicar a estrutura de blockchain e como a mempool armazena transações em sequência;
- Relacionar a estrutura da blockchain com sequências numéricas e progressões;
- Ensinar a classificar progressões aritméticas e identificar suas características;

- Determinar o termo geral de uma PA e aplicá-lo na análise de recompensas em *Bitcoin*;
- Promover a resolução de problemas práticos que envolvam PA, especialmente em cenários de mineração;
- Introduzir a classificação e o termo geral das progressões geométricas;
- Relacionar PG às recompensas de Bitcoin a cada bloco minerado, demonstrando a aplicação matemática;
- Discutir o conceito do limite total de Bitcoin que pode ser minerado, conectando matemática e tecnologia.

Recursos:

- Quadro branco e lápis;
- Projetor Multimídia e Notebooks;
- Computadores e Celulares.

3.1.1 Aula 1 — Introdução a sequências numéricas, elementos de uma sequência, recorrência e termo geral.

- Tempo estimado: 2 aulas de 50 min.
  - Momento I: 1 aula (50 min).
  - Momento II: 1 aula (50 min).
- Desenvolvimento:
  - Momento I: Inicie a aula escrevendo no quadro ou apresente em slides os seguintes números:

    $$\mathbf{1, 1, 2, 3, 5, 8, 13, \_\_\_\_\_}$$

    Questione os alunos: Alguém sabe qual é o próximo número dessa lista? Como podemos descobrir?

    Dê um tempo para que os alunos observem e formulem hipóteses em duplas ou pequenos grupos. Circule entre os estudantes, escutando suas ideias e incentivando o debate. Após alguns minutos, peça que alguns compartilhem suas respostas com a turma. Caso necessário, ofereça pistas que levem à descoberta do padrão, como: O que acontece se somarmos dois números vizinhos?

Conduza a turma à conclusão de que cada número é a soma dos dois anteriores, caracterizando a sequência de Fibonacci. Escreva no quadro:

$$\mathbf{1 + 1 = 2, \quad 1 + 2 = 3, \quad 2 + 3 = 5, \quad \ldots}$$

Após a identificação do padrão, introduza formalmente o conceito de sequência numérica, utilizando uma linguagem acessível. Explique que: na matemática, uma sequência é como uma lista ordenada de números, em que cada número ocupa uma posição específica. Por exemplo: 2, 4, 6, 8, 10... é uma lista onde cada termo soma 2 ao anterior. Apresente os termos técnicos com clareza:

* **Termo:** cada número da sequência;
* **Ordem:** a posição que o número ocupa;
* **Lei de formação:** a regra que define como a sequência se forma.

Mostre outros exemplos simples no quadro:

* Sequência dos múltiplos de 5: 5, 10, 15, 20...
* Sequência decrescente: 100, 90, 80, 70...
* Sequência alternada: 1, -1, 1, -1...

Pergunte aos alunos: Essas listas seguem alguma regra? Todas têm uma ordem definida?

Finalize com a definição:

Definição 3.1. *Uma **sequência numérica** é uma função cujo domínio é o conjunto dos números naturais* $\mathbb{N}$*, no caso de sequências infinitas, ou o conjunto* $\{1, 2, \ldots, n\}$*, no caso de sequências finitas com* n *elementos. O contradomínio da função é o conjunto dos números reais* $\mathbb{R}$*.*

– Momento II: Explique com exemplos que cada sequência pode ser determinada por:

  * **Lei de formação (ou termo geral):** quando é possível encontrar uma fórmula que determina qualquer termo da sequência, a partir da sua ordem.
  * **Relação de recorrência:** quando cada termo depende de um ou mais termos anteriores.

  Utilize a sequência de Fibonacci como exemplo de recorrência:

$$a_1 = 1, \quad a_2 = 1, \quad a_n = a_{n-1} + a_{n-2}, \quad \text{para } n \geq 3$$

E mostre uma sequência com termo geral, como:

$$a_n = 2n, \quad \text{que gera: } 2, 4, 6, 8, 10, \ldots$$

Apresente aos alunos os dois principais tipos de sequências quanto à quantidade de termos:

* **Sequência finita:** possui um número determinado de termos (ex: 1, 2, 3, 4).
* **Sequência infinita:** seus termos se prolongam indefinidamente (ex: 1, 2, 3, 4, 5, 6, ...).

Escreva no quadro exemplos diversos para discussão:

* Sequência par: $a_n = 2n$
* Sequência ímpar: $a_n = 2n - 1$
* Sequência quadrática: $a_n = n^2$

Promova perguntas aos alunos: Qual é o 10º termo dessa sequência? E o 20º? Isso ajuda os estudantes a entenderem o papel da fórmula do termo geral como uma ferramenta eficiente para prever valores em qualquer posição da sequência.

Para fixação, proponha uma atividade no quadro: peça aos alunos que, em duplas, criem uma sequência que possa ser definida por termo geral e outra por recorrência. Oriente que tentem escrever a regra de formação e compartilhem com a turma.

Esse momento visa formalizar os conceitos fundamentais que sustentam os estudos futuros sobre progressões aritméticas e geométricas, dando aos alunos uma base sólida e organizada para as próximas aulas.

- Resultados Esperados Qualitativos:

  – Espera-se que os alunos se empolguem com a introdução inicial da sequência de Fibonacci, buscando formas de encontrar seu próximo termo e com uso do termo lista facilite a compreensão e associação de uma sequência. Além disso, espera-se que os alunos possam ter contato com a história da Matemática.

3.1.2 Aula 2 — Introdução à rede *Bitcoin*, *mempool* do *Bitcoin* e como ela é formada por uma sequência de blocos e transações.

- Tempo estimado: 2 aulas de 50 min.
  - Momento I: 1 aula (50 min).
  - Momento II: 1 aula (50 min).
- Desenvolvimento:
  - Momento I: Abrir um diálogo inicial com os alunos questionando: O que é o *Bitcoin*. Incentivar que compartilhem o que já ouviram falar ou sabem sobre o tema, valorizando as experiências prévias. Em seguida, apresentar os conceitos iniciais sobre a rede *Bitcoin*. Mostrar aos alunos a blockchain em tempo real no site: https://mempool.space/pt/. Propor uma dinâmica prática: organizar os alunos em filas, representando os blocos da Rede *Bitcoin*. O professor envia mensagens criptografadas aos últimos alunos de cada fila, utilizando um algoritmo simples de substituição (por exemplo, número → letra). Apenas o professor e o último aluno da fila conhecem o método de criptografia. O objetivo é que o último aluno decifre e leia a mensagem, demonstrando a segurança da criptografia e a estrutura sequencial dos blocos.
  - Momento II: Iniciar uma sequência de atividades que relacionam diretamente o funcionamento da Rede *Bitcoin* com conceitos matemáticos de sequência. Apresenta-se, a seguir, uma sugestão de questões para este exercício.

Quadro 3 – Aula 2: Exercícios

AULA 2 - EXERCÍCIOS

QUESTÃO 1 - A Rede *Bitcoin* é uma sequência?
QUESTÃO 2 - A Rede *Bitcoin* é uma sequência finita ou infinita de blocos?
QUESTÃO 3 - Vimos que a Rede *Bitcoin* recompensa o minerador a cada bloco e, a cada ciclo de 210 mil blocos, essa recompensa é reduzida pela metade. O primeiro ciclo recompensava com 50 BTC. Qual será a recompensa após 4 ciclos?

Fonte: Elaborado pelo próprio autor.

- Resultados Esperados Qualitativos:
  - Espera-se que os alunos se envolvam com a abordagem interdisciplinar, percebendo a aplicação direta da matemática em um tema atual e tecnológico.

A dinâmica com a criptografia, aliada ao uso de recursos digitais e problemas contextualizados, deve despertar a curiosidade e promover o desenvolvimento do raciocínio lógico e matemático. Através das discussões e resoluções de problemas, os alunos devem ser capazes de compreender conceitos como sequência, progressão geométrica e finitude, ampliando sua capacidade de abstração e análise crítica sobre sistemas digitais.

3.1.3 Aula 3 — Progressão Aritmética, classificação da PA, termo geral da PA e PA na rede Bitcoin.

- Tempo estimado: 2 aulas de 50 min.
  - Momento I: 1 aula (50 min).
  - Momento II: 1 aula (50 min).
- Desenvolvimento:
  - Momento I: Iniciar a aula com uma situação-problema contextualizada do cotidiano e iscutir com os alunos as estratégias de resolução. Resolver o problema com os alunos e propor outros exemplos práticos semelhantes, reforçando o reconhecimento da PA em situações do dia a dia. Apresenta-se, a seguir, uma sugestão de questão.

Quadro 4 – Aula 3: Exercícios

AULA 3 - EXERCÍCIOS

QUESTÃO 1 - Emerson plantou uma muda de árvore em seu jardim. No primeiro mês, a planta cresceu 5 centímetros. A cada mês seguinte, a planta cresce 3 centímetros a mais do que no mês anterior.

a) Qual será a altura da planta ao final de 6 meses?

b) Qual a altura da planta no $10^{\underline{o}}$ mês?

Fonte: Elaborado pelo próprio autor.

E, em seguida, apresentar formalmente o conceito de Progressão Aritmética, destacando os elementos. Apresente no quadro ou nos slides a definição:

Definição 3.2. ***Progressão Aritmética*** *é uma sequência onde a diferença entre cada termo e o termo anterior é constante. Essa diferença constante é chamada de razão da progressão e é representada pela letra* r.

Explique os principais elementos de uma PA:

∗ a_1: primeiro termo;

∗ r: razão (diferença comum entre os termos);

∗ a_n: enésimo termo;

∗ n: número da posição (ordem) do termo.

Apresente a fórmula do termo geral da PA:

$$a_n = a_1 + (n-1)r.$$

Utilize um exemplo simples para ilustrar:

Considere a PA: 5, 8, 11, 14, ... Aqui, $a_1 = 5$ e $r = 3$. Logo, $a_4 = 5 + (4-1) \cdot 3 = 14$.

– Momento II: Apresentar problemas aplicando o conceito de PA no contexto da rede *Bitcoin*, estimulando o raciocínio lógico, abstração e associação entre uma PA e as transações na rede. Apresenta-se, a seguir, umas sugestões de questões.

Quadro 5 – Aula 3: Exercícios

AULA 3 - EXERCÍCIOS

QUESTÃO 1 - Os blocos da Rede Bitcoin formam uma PA? Se sim, qual é a razão?
QUESTÃO 2 - Do bloco 420100 ao bloco 420104, as transações formam uma PA? Se sim, qual a razão?
QUESTÃO 3 -Em um determinado mês, a rede Bitcoin processou 200 transações no primeiro bloco. A cada bloco seguinte, o número de transações aumentou em 50. Qual será o número de transações processadas no 5º bloco?
QUESTÃO 4 -Suponha que a rede Bitcoin comece com 300 transações no primeiro bloco. Se o número de transações diminui em 20 a cada bloco, quantas transações haverá no 10º bloco?

Fonte: Elaborado pelo próprio autor.

- Resultados Esperados Qualitativos:

  – Espera-se que os alunos aprofundem sua compreensão sobre progressão aritmética, reconhecendo seus elementos e aplicando-os com segurança em problemas contextualizados. A associação entre conteúdos matemáticos e o funcionamento da rede *Bitcoin* deve fortalecer o entendimento da PA como uma ferramenta útil na modelagem de fenômenos reais e tecnológicos. Com a exploração de situações com razões positivas e negativas, os alunos também deverão desenvolver maior flexibilidade cognitiva e pensamento analítico, habilidades essenciais para o aprendizado matemático e a resolução de problemas.

3.1.4 Aula 4 — Soma da Progressão Aritmética.

- Tempo estimado: 1 aula de 50 min.
  - Momento I: 25 min.
  - Momento II: 25 min.
- Desenvolvimento:
  - Momento I: Iniciar a aula com uma situação-problema exploratória, escrita no quadro ou projetada. Propor que os alunos discutam em duplas ou pequenos grupos e explorem estratégias próprias de contagem, agrupamento ou estimativa. Incentivar o uso de ideias como: Pareamento de termos (ex: 1+100, 2+99, 3+98...). Apresenta-se, a seguir, uma sugestão de questão.

Quadro 6 – Aula 4: Exercícios

AULA 4 - EXERCÍCIOS
QUESTÃO 1 - Qual a soma de 1 até 100? E de 1 até 1000?

Fonte: Elaborado pelo próprio autor.

  - Momento II: Apresentar e formalizar a fórmula da soma dos termos da PA e resolver o problema utilizando essa fórmula. Apresente a fórmula no quadro ou em slides:

$$S_n = \frac{n}{2} \cdot (a_1 + a_n).$$

    Explique que essa fórmula calcula a soma dos n primeiros termos de uma PA, onde:
    * S_n: soma dos n primeiros termos;
    * a_1: primeiro termo da PA;
    * a_n: último termo (ou termo de ordem n);
    * n: número de termos a serem somados.
- Resultados Esperados Qualitativos:

  Espera-se que os alunos desenvolvam estratégias autônomas de resolução de problemas, compreendendo padrões e regularidades antes da introdução formal da fórmula da soma da PA. Ao final da aula, espera-se que consigam aplicar a fórmula corretamente e interpretar os resultados em contextos variados, consolidando a associação entre conteúdos matemáticos e fenômenos reais. A aula também visa promover a transição do pensamento aritmético para o pensamento algébrico, além de fortalecer a compreensão conceitual da estrutura das progressões.

3.1.5 Aula 5 — Progressão Geométrica, classificação, termo geral da PG. Recompensas em BTC a cada bloco.

- Tempo estimado: 2 aulas de 50 min.
  - Momento I: 1 aula (50 min).
  - Momento II: 1 aula (50 min).
- Desenvolvimento:
  - Momento I: Iniciar a aula com uma situação-problema contextualizada. Propor que os alunos identifiquem o padrão de crescimento nos valores e testem estratégias próprias para prever o valor economizado no 4º mês e a soma acumulada. Em seguida, apresentar o conceito de Progressão Geométrica (PG), sua representação por meio do termo geral, e trabalhar com exemplos simples. Apresenta-se, a seguir, uma sugestão de questão.

Quadro 7 – Aula 5: Exercícios

AULA 5 - EXERCÍCIOS

QUESTÃO 1 - Emerson começou a economizar para comprar um celular. No primeiro mês, ela economizou 50 reais, e a cada mês seguinte, o valor economizado foi o dobro do mês anterior.

a) Qual será o valor que Emerson economizará no 4º mês?

b) Qual é o total economizado ao final de 4 meses?

Fonte: Elaborado pelo próprio autor.

Escreva no quadro ou apresente em slides o conceito de Progressão Geométrica (PG), sua representação por meio do termo geral:

Definição 3.3. *Uma **Progressão Geométrica** é uma sequência numérica da forma*

$$(a_1, a_2, a_3, \ldots),$$

em que, a partir do segundo termo, cada termo é obtido pela multiplicação do termo anterior por uma constante q, chamada de razão da PG. Isto é, para todo $n \geq 2$, vale:

$$a_n = a_{n-1} \cdot q.$$

Apresente a **fórmula do termo geral da PG**:

$$a_n = a_1 \cdot q^{n-1}.$$

Onde:

- a_n: é o termo de ordem n;
- a_1: é o primeiro termo da PG;
- q: é a razão da PG;
- n: é a posição (ordem) do termo na sequência.

- Momento II: Relacionar a Progressão Geométrica com o mecanismo de funcionamento da política monetária do *Bitcoin*, especialmente com a recompensa por bloco minerado. Explique que, desde sua criação, a política monetária do *Bitcoin* estabelece que a recompensa por bloco é reduzida à metade a cada ciclo de aproximadamente **210 mil blocos**, processo conhecido como *halving*. Isso forma uma PG decrescente com:

  - $a_1 = 50$ BTC (recompensa inicial);
  - $q = \frac{1}{2}$ (razão da PG, pois a recompensa é reduzida pela metade a cada ciclo).

    Ressalte aos alunos que esse processo garante um controle da oferta de moedas e evita a inflação, funcionando como uma espécie de política monetária programada.

    Após a contextualização, proponha a resolução de problemas aplicando o conceito de PG no contexto da rede *Bitcoin*, estimulando o raciocínio lógico, abstração e associação entre uma PG e a política monetária da rede. Oriente os alunos a identificarem as variáveis da PG em cada problema, aplicar a fórmula do termo geral, justificar seus raciocínios e interpretar os resultados. Apresenta-se, a seguir, umas sugestões de questões.

Quadro 8 – Aula 5: Exercícios

AULA 5 - EXERCÍCIOS

QUESTÃO 1 - O primeiro ciclo recompensava o minerador em 50 BTC. Em 8 ciclos, qual será a recompensa por bloco minerado?
QUESTÃO 2 - O primeiro ciclo recompensava o minerador em 50 BTC. Em quantos ciclos a recompensa por bloco será de 3,125 BTC?
QUESTÃO 3 - O primeiro ciclo recompensava o minerador em 50 BTC. Sabendo que 210 mil blocos são processados em aproximadamente 4 anos, em quantos anos a recompensa por bloco minerado será de 6,25 BTC?

Fonte: Elaborado pelo próprio autor.

- Resultados Esperados Qualitativos:

  Espera-se que os alunos identifiquem e compreendam situações que envolvam Progressão Geométrica, reconhecendo o padrão multiplicativo entre os termos de uma sequência. Ao aplicar esse conhecimento ao contexto da rede do Bitcoin, os alunos devem perceber como a redução da recompensa por bloco representa um exemplo real de PG, com implicações tecnológicas e econômicas. As atividades também favorecem o desenvolvimento do pensamento lógico, multiplicativo e algébrico, além de integrar matemática a temas de relevância contemporânea. Ao final da aula, espera-se que os alunos estejam preparados para formalizar e aplicar a fórmula do termo geral da PG e interpretar seu significado em diferentes contextos.

3.1.6 Aula 6 — Soma dos termos de uma PG finita, soma dos termos de uma PG infinita, soma de unidades de BTC por ciclos; limite total de BTC possível de ser minerado.

- Tempo estimado: 2 aulas de 50 min.
  - Momento I: 1 aula (50 min).
  - Momento II: 1 aula (50 min).
- Desenvolvimento:
  - Momento I: Iniciar a aula com uma situação-problema contextualizada. Propor que os alunos identifiquem qual a soma dos valores e testem estratégias próprias para prever o valor total. Apresenta-se, a seguir, uma sugestão de questão.

Quadro 9 – Aula 6: Exercícios

AULA 6 - EXERCÍCIOS
QUESTÃO 1 - Emerson está planejando uma série de investimentos em renda fixa. No primeiro mês, ele investe R$ 1.000,00 e dobra o valor investido a cada mês subsequente. Considerando que ele continuará por 6 meses, qual será o total investido nesse período?

Fonte: Elaborado pelo próprio autor.

Em seguida, apresentar a fórmula da soma dos n primeiros termos de uma PG finita e infinita. Explique que a PG finita possui número limitado de termos e é comum em contextos como investimentos, parcelas ou ciclos de tempo definidos. Já a PG infinita é utilizada em situações onde a sequência continua indefinidamente, com razão entre -1 e 1.

Soma dos n primeiros termos de uma PG finita:

Apresente a fórmula:

$$S_n = a_1 \cdot \frac{q^n - 1}{q - 1}, \quad \text{para } q \neq 1$$

Explique os elementos:

* S_n: soma dos n primeiros termos;
* a_1: primeiro termo;
* q: razão da PG;
* n: número de termos a serem somados.

Exemplo:

> *O primeiro ciclo do Bitcoin recompensa com 50 BTC. Quantos bitcoins são minerados ao final de 4 ciclos?*

Utilize: $a_1 = 50$, $q = \frac{1}{2}$, $n = 4$

$$S_4 = 50 \cdot \frac{\left(\frac{1}{2}\right)^4 - 1}{\frac{1}{2} - 1} = 50 \cdot \frac{\frac{1}{16} - 1}{-\frac{1}{2}} = 50 \cdot \frac{-\frac{15}{16}}{-\frac{1}{2}} = 50 \cdot \frac{15}{8} = 93{,}75 \text{ BTC}$$

Conclua explicando que um ciclo tem 210 mil blocos e basta multiplicar os 93,75 BTC por 210000 e encontrará o total nesses quatro ciclos (19687,5 BTC), e que este valor representa a soma decrescente das recompensas por bloco ao longo do tempo.

Soma de uma PG infinita:

Apresente a fórmula:

$$S = \frac{a_1}{1 - q}, \quad \text{com } |q| < 1$$

Explique que essa fórmula é válida somente para PGs infinitas com razão entre -1 e 1, como é o caso da política de emissão do*Bitcoin*.

– Momento II: Apresentar e aplicar o conceito de soma de PG ao funcionamento da rede do *Bitcoin*, em especial no modelo de recompensa decrescente por bloco a cada ciclo.

Quadro 10 – Aula 6: Exercícios

AULA 6 - EXERCÍCIOS

QUESTÃO 1 - O primeiro ciclo recompensava o minerador com 50 BTC. Sabendo que 210 mil blocos são minerados em cada ciclo, responda:

a) Quantos BTC serão minerados em 2 ciclos?

b) E em 4 ciclos?

QUESTÃO 2 - Considerando que a recompensa do Bitcoin reduz pela metade a cada ciclo (50, 25, 12,5, ...), qual será o total de BTC que pode ser minerado?

Fonte: Elaborado pelo próprio autor.

- Resultados Esperados Qualitativos:
  - Espera-se que os alunos reconheçam e apliquem a fórmula da soma de uma Progressão Geométrica finita e infinita, com compreensão conceitual do comportamento exponencial da sequência. Ao relacionar com investimentos e mineração de Bitcoin, os alunos devem entender que a PG modela situações reais e complexas, como o crescimento de capital ou a política de emissão monetária. Essa aula favorece o desenvolvimento do pensamento algébrico avançado, raciocínio financeiro e interpretação crítica de dados numéricos.

4 Conclusões

A utilização da rede *Bitcoin* e da visualização da *blockchain* por meio do site mempool.space representa uma oportunidade inovadora de promover a aprendizagem significativa de sequências e progressões. Ao aproximar os conteúdos matemáticos da realidade digital dos estudantes, essa proposta favorece a motivação, a contextualização e o desenvolvimento de competências essenciais previstas na BNCC. A abordagem permite que os alunos associem conceitos abstratos a estruturas reais, como o crescimento controlado da oferta de *bitcoins*, consolidando a matemática como ferramenta de leitura crítica do mundo contemporâneo.

Esperamos, com esta proposta, contribuir para a valorização do ensino da matemática em contextos significativos, ampliando a percepção dos alunos sobre sua aplicabilidade e promovendo a articulação entre o conteúdo matemático e os avanços tecnológicos da sociedade contemporânea. Ao final da sequência, os estudantes deverão ser capazes de compreender e aplicar os conceitos de PA e PG, interpretar situações envolvendo crescimento e decaimento exponencial e refletir criticamente sobre o papel da matemática na organização de sistemas complexos como o *Bitcoin*.

Referências

MACEDO, R. A. A. *Sistemas Lineares e Métodos Numéricos: uma proposta para o Ensino Médio*. Dissertação (Trabalho de Conclusão de Curso (Mestrado em Matemática)) — Universidade Federal de Campina Grande, Campina Grande, PB, 2023. Acesso em: 04 mês ano. Disponível em: <https://sca.profmat-sbm.org.br/profmat_tcc.php?id1=7179&id2=171055870>. Citado na página 11.

MARQUES, C. P. *A importância da Análise Real na formação do Professor de Matemática do Ensino Médio: o caso das sequências numéricas*. Dissertação (Dissertação (Mestrado)) — PROFMAT, Universidade Federal de Campina Grande (UFCG), 2019. Citado na página 10.

NAKAMOTO, S. *Bitcoin: um sistema de dinheiro eletrônico peer-to-peer*. 2008. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 30 ago 2024. Citado 2 vezes nas páginas 4 e 7.

SOUZA, B. V. d. *Problemas do 2º grau: uma proposta de sequências didáticas sob a perspectiva da metodologia de resolução de problemas*. Dissertação (Dissertação (Mestrado em Matemática)) — Universidade Federal de Campina Grande, Centro de Ciências e Tecnologia, Campina Grande, 2023. Orientação: Prof. Dr. Leomaques Francisco Silva Bernardo. 142 f. : il. color. Citado na página 11.

ZABALA, A. *A prática educativa : como ensinar [recurso eletrônico]*. [S.l.]: Editora ABDR, 1998. Citado na página 11.