Blockchain em Sistema Eleitoral

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Curso Superior de Tecnologia em Segurança da Informação pelo Centro Paula Souza – FATEC Faculdade de Tecnologia de Americana – Ralph Biasi.
Área de concentração: Ciberseguranca.

Americana, 01 de dezembro de 2022

Banca Examinadora:

Maxwel Vitorino da Silva (Presidente)
Mestre
FATEC Faculdade de Tecnologia de Americana

Renato Kraide Soffner (Membro)
Doutor
FATEC Faculdade de Tecnologia de Americana

Ivan Menerval da Silva (Membro)
Doutor
FATEC Faculdade de Tecnologia de Americana

Blockchain em Sistema Eleitoral

Gabriel da Mata Dias

Maxwel Vitorino da Silva

Curso Superior de Tecnologia em Segurança da Informação – Faculdade de Tecnologia de Americana (FATEC Americana) "Ministro Ralph Biasi"
Americana – SP - Brasil

gabriel.dias7@fatec.sp.gov.br

maxwel.silva5@fatec.sp.gov.br

Abstract. *Due to the advancement and use of digital media in our daily lives, cyber criminals with malicious intent to steal, alter, destroy data and information also appear as a side effect, thus making a generalized lack of confidence in technological means inevitable, this article aims and focuses on proposing a modern model of an electoral voting system that meets information security requirements such as reliability, integrity, availability and hindering cyber-attacks, for which the use of blockchain, conceptual concepts was analyzed of information security, cryptography concepts like hashs.*

Resumo. *Devido ao avanço e utilização dos meios digitais em nossos dia a dia, surge-se também como um efeito colateral cyber criminosos com intenções maliciosos de roubar, alterar, destruir dados e informações, tornando-se assim inevitável uma generalizada falta de confiança nos meios tecnológicos, o presente artigo tem como objetivo e foco propor um modelo moderno de um sistema de votação eleitoral que atenda aos requisitos da segurança da informação como a confiabilidade, integridade, disponibilidade e dificultar cyber ataques, para isso foi analisado o uso de blockchain, múltiplos conceitos de segurança da informação, conceitos de criptografia como hashs.*

1. Introdução

A utilização de tecnologias digitais em processos eleitorais tem se tornado cada vez mais comum em todo o mundo. No entanto, a crescente preocupação com a integridade e confiabilidade desses sistemas tem sido um desafio global enfrentado por empresas, organizações, governos e indivíduos.

No Brasil, a desconfiança da população no sistema eleitoral utilizado nas eleições de 2022 é evidente, assim como em outros países como os Estados Unidos. A falta de confiança e segurança é um dos principais obstáculos para a implementação de um sistema eleitoral totalmente digital.

Neste trabalho, propõe-se a utilização do conceito de blockchain e criptografia para solucionar esses problemas e garantir a integridade e confiabilidade do processo eleitoral. O objetivo deste estudo é analisar como o uso da tecnologia blockchain pode contribuir para a segurança e confiabilidade dos sistemas eleitorais digitais, diminuindo a desconfiança da população e aumentando a transparência e eficiência do processo eleitoral.

2. Seguranca da Informacao

Define-se Segurança da Informação:

> "O termo segurança da informação pode ser designado como uma área do conhecimento que salvaguarda os chamados ativos da informação, contra acessos indevidos, modificações não autorizadas ou até mesmo sua não disponibilidade" (Peixoto, 2006, p. 37).

A segurança da informação é uma área do conhecimento que visa proteger os ativos da informação contra acessos indevidos, modificações não autorizadas ou até mesmo sua não disponibilidade.

O valor de uma informação está na visão de quem a possui, de acordo com Mitnick e Simon (2003, p. 21), "Assim como as peças de um quebra-cabeça, cada informação parece irrelevante sozinha. Porém, quando as peças são juntadas, uma figura aparece." e, quando colocada nas mãos corretas, pode se tornar uma poderosa ferramenta ou arma.

A segurança da informação é fundamental em qualquer entidade organizacional e possui três pilares básicos:

- Confidencialidade: garante que as informações transmitidas chegarão ao seu destino sem se dissiparem para outro lugar.

- Integridade: garante que as informações não sofram modificações durante o trajeto entre a pessoa que enviou e a pessoa que recebeu a informação, garantindo sua veracidade.

- Disponibilidade: garante que as informações estarão sempre disponíveis para serem utilizadas.

Assegurar a segurança da informação é fundamental para garantir a confiabilidade das informações e proteger as entidades organizacionais contra ameaças cibernéticas.

Conforme demonstrado na Figura 1.

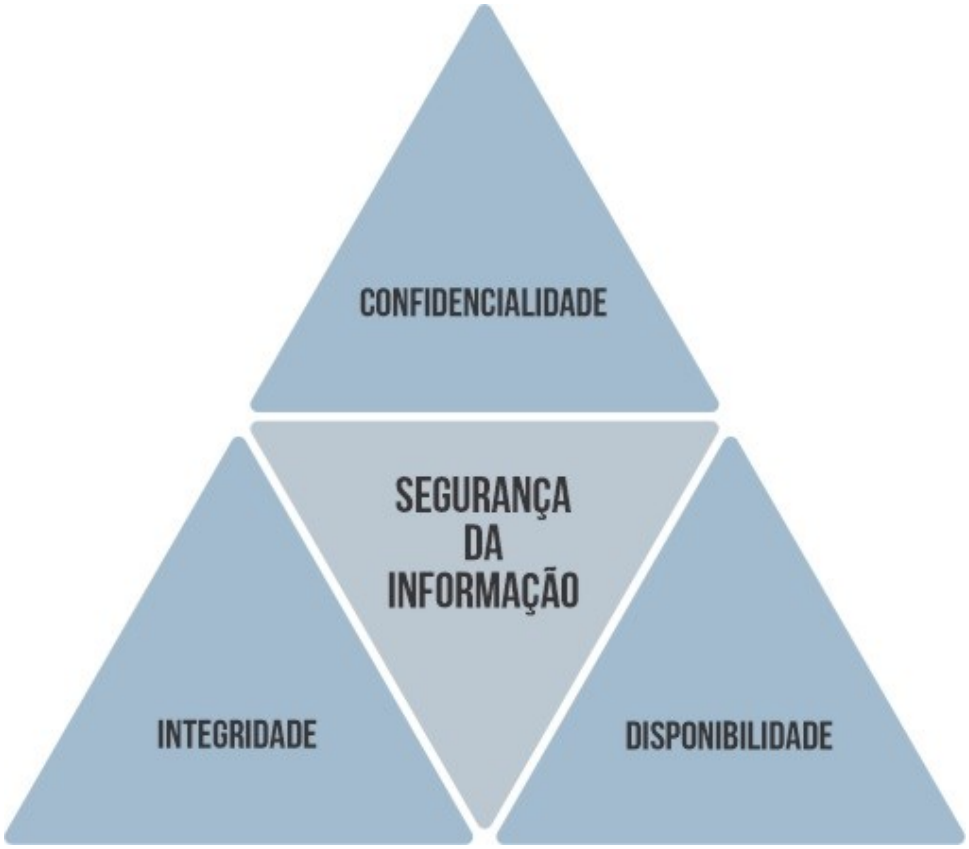

Figura 1 – Pilares Segurança da Informação.

Fonte: medium.com, 2022

2.1. Criptografia

A criptografia é a ciência que utiliza algoritmos matemáticos para proteger informações confidenciais. Inicialmente, a criptografia clássica utilizava canetas e papéis para cifrar mensagens, mas com o avanço da tecnologia, a criptografia moderna surgiu, trazendo novas ferramentas e conceitos como a Enigma Machine, desenvolvida pelos alemães durante a Segunda Guerra Mundial, e algoritmos de *Hash* criptográfica utilizados em meios digitais.

Hoje em dia, a criptografia é considerada um dos principais mecanismos de

segurança no meio digital, sendo utilizada para garantir a proteção contra o vazamento de dados. A criptografia tem sido objeto de uma corrida armamentista contínua, onde uma das partes busca novas formas de cifrar informações e a outra busca formas rápidas e eficientes de quebrar essas criptografias.

De acordo com Mendes, Paulicena, Souza (2011) a criptografia é a ciência de utilizar algoritmos (cálculos matemáticos) para ofuscar uma informação, sendo considerada um dos principais mecanismos de segurança no meio digital, usada para garantir a proteção contra os riscos associados a vazamento de dados.

Com o avanço da criptografia e a capacidade de cifrar dados e informações, iniciou-se uma corrida armamentista que ainda dura até os dias de hoje, onde uma das partes busca novas e melhores formas de cifrar informações, enquanto a outra procura formas rápidas e eficientes de quebrar essas criptografias.

Uma das ferramentas atualmente utilizadas para garantir a segurança de uma informação e a função *hash*, também conhecida por função resumo, soma *hash* ou *checksum*, trabalha recebendo uma entrada de tamanho variável e com característica de retornar uma sequência de caracteres hexadecimais de tamanho fixo, independentemente do tamanho de sua entrada, *hashes* são utilizadas como validadoras de integridade de arquivos e informações.

Caso a entrada de uma *hash* seja alterada em um bit, o vsalor da *hash* sofrerá mudanças apontando sua alteração assim uma função *hash* criptográfica consegue fornecer uma garantia da integridade dos dados inseridos na mesma.

Utilizada em sistemas bancárias, jurídicos e *e-commerces*, *hashs* não possuem a característica de serem invioláveis, mas sua ampla utilização e devido o tempo necessário que irá ser gasto na tentativa de quebra de uma *hash* sendo este intervalo em casos específicos maiores que o tempo de vida de um indivíduo.

De "S*ecure hash algorithm*" e "256" para 256 bytes, temos que a *SHA256* uma função *hash* projetada pela *NSA* (Agência de Segurança Nacional dos EUA) sendo então publicado pela primeira vez em 2001 e em 2002 a família SHA2 se tornou o novo "Padrão de *Hash* Seguro".

Sendo utilizada em aplicações de segurança e protocolos amplamente utilizados, como processo de autenticação de pacotes de softwares *Debian GNU/Linux e* empregada em múltiplas criptomoedas como Bitcoin, além de ser exigidos por lei no uso de certas aplicações do Governo dos Estados Unidos da América.

INPUT DATA	HASH OUTPUT (SHA-256)
My name is Toby	cacb5418163039b016be9746818a2926f68fd1e4bad1b04f6791f6aabb5e8c52
My name is Tony	9cd2444dc56929bdb97123add1f007643effa88bf1ed061eee1ead4e15ac7f9
My name is Toby and this is my project	9abbaa0c54fcd028ac51bede2608d06e8d3a026784e34adfac14fadd143d212c

Figura 2. Exemplo SHA256.

Fonte: medium.com, 2022

3. Blockchain

Para entender o porquê de se usar uma *blockchain*, é preciso primeiro entender o que é categoriza uma *blockchain*. De acordo com Santos, Prata, Araujo (2019) *blockchain* pode-se definido como um banco de dados que armazena dados em blocos (Block) ligados em uma cadeia ou corrente (Chain).

Blocos possuem em si registro de informações que devem ser inseridos na corrente, o primeiro bloco chamado Bloco Genesis (*Genesis Block*) serve-se como o estado inicial do sistema, todos blocos subsequentes irão possuir uma *hash* criptografada de seus dados e a *hash* de seu antecessor formando se assim a corrente, conforme mostrado na Figura 3.

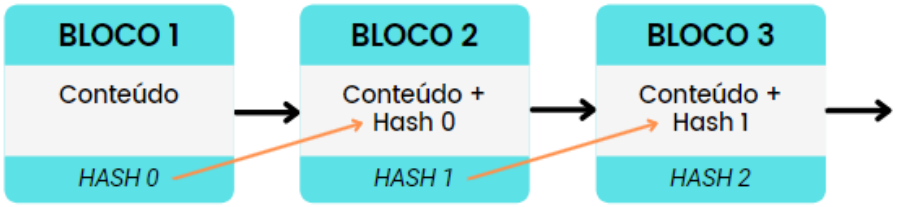

Figura 3. Blockchain

Fonte: talura.io, 2022

Blockchain como um todo possui uma rede descentralizada consistindo em múltiplos nós de cópias exatas dos blocos publicados, para evitar erros de confiabilidade são utilizados algoritmos de consenso como *Proof of Work* (PoW).

PoW è a validação mais utilizada em redes *blockchain* requerendo que o nó que deseje inserir um bloco na cadeia necessite calcular uma *hash* correspondente as condições impostas pela rede.

Cada bloco é validado por um consenso entre os participantes da rede, garantindo sua integridade e impedindo a alteração de dados já registrados. Essa validação é feita por meio de criptografia, utilizando chaves públicas e privadas.

Além de registrar transações financeiras, o blockchain pode ser utilizado para armazenar quaisquer tipos de dados, como contratos, registros médicos ou até mesmo votos em eleições. Sua descentralização e segurança tornam a tecnologia atraente para aplicações em diversos setores.

3.1. Vantagens e Desvantagens

De acordo com a *Binance* (2022) as vantagens e desvantagens da utilização de uma blockchain são:

- Distribuído: Como os dados da Blockchain costumam ser armazenados em milhares de dispositivos numa rede distribuída de nodes (nós), o sistema e esses dados são altamente resistentes à falhas técnicas e ataques maliciosos. Cada node na rede é capaz de replicar e armazenar uma cópia do banco de dados, por esse motivo

não há ponto central de falha: um único node que fica off-line não afeta a disponibilidade ou a segurança da rede. Por outro lado, muitos bancos de dados convencionais dependem de um servidor único ou somente alguns, por isso são mais vulneráveis à falhas técnicas e ataques maliciosos.

- Estabilidade: É muito improvável que blocos confirmados sejam revertidos posteriormente, significando que, uma vez registrados que os dados são registrados na Blockchain, é extremamente difícil removê-los ou alterá-los. Isso faz da Blockchain uma ótima tecnologia para armazenar registros financeiros ou quaisquer outros dados em que uma auditoria possa ser necessária, pois todas as alterações são rastreadas e permanentemente registradas em um livro distribuído e público. Por exemplo, uma empresa pode usar a tecnologia Blockchain para impedir ações fraudulentas de seus funcionários. Nesse cenário, a Blockchain pode fornecer um registro seguro e estável de todas as transações financeiras que ocorrem dentro da empresa. Isso dificultaria a tentativa de um funcionário esconder transações suspeitas.
- Sistema *Trustless*: Na maioria dos sistemas de pagamento tradicionais, as transações não dependem apenas das duas partes envolvidas, mas também de um intermediário - como um banco, empresa de cartão de crédito ou provedor de pagamento. Ao usar a tecnologia Blockchain, todo esse arranjo não é mais necessário porque a rede distribuída de nodes verifica as transações por meio de um processo conhecido como mineração. Por essa razão, a *Blockchain* é usualmente conhecida como um sistema "*Trustless*". Portanto, um sistema Blockchain elimina o risco de confiar em uma única organização, reduz os custos gerais e as taxas das transações, cortando intermediários e terceiros.
- Ataques de 51%: O algoritmo de consenso *Proof of Work* (PoW) que protege a *Blockchain* do *Bitcoin* provou ser muito eficiente ao longo do tempo. No entanto, existem alguns ataques em potencial que podem ser realizados contra redes *Blockchain*, dentre eles está o Ataque de 51%. Tal ataque pode acontecer se uma organização conseguir controlar mais que 50% do poder computacional da rede, permitindo que eles interfiram no funcionamento da rede excluindo ou modificando intencionalmente a ordenação das transações. Apesar de ser teoricamente possível, nunca houve um Ataque de 51% bem-sucedido na rede *Blockchain* do *Bitcoin*. À medida que ela cresce, a segurança aumenta e é muito improvável que os mineradores invistam grandes quantias de dinheiro e recursos para atacar o *Bitcoin*, já que são mais bem recompensadas por trabalhar honestamente. Além disso, um Ataque de 51% bem-sucedido só seria capaz de modificar as transações mais recentes por um curto período de tempo, porque os blocos são vinculados através de provas criptográficas (mudar blocos mais antigos exigiria níveis intangíveis de poder computacional). Além disso, a *Blockchain* do *Bitcoin* é muito resiliente e se adapta rapidamente em resposta a um ataque.
- Modificação de Informações: Outra desvantagem dos sistemas *Blockchain* é que, uma vez que os dados foram adicionados à rede, é muito difícil modificá-los. Embora a estabilidade seja uma das vantagens da Blockchain, nem sempre é uma boa característica. Alterar dados ou o código de uma rede *Blockchain* é normalmente muito complicado e geralmente requer um *Hard Fork* (Bifurcação), onde uma

cadeia de blocos é abandonada e outra é criada.

- Chaves Privadas: A *Blockchain* usa criptografia de chave pública (ou assimétrica) para dar aos usuários a propriedade sobre suas criptomoedas (ou quaisquer outros dados da Blockchain). Cada conta (ou endereço) na Blockchain tem duas chaves correspondentes: uma chave pública (que pode ser compartilhada) e uma chave privada (que deve ser mantida em segredo). Os usuários precisam da chave privada para acessar seus fundos, significando que eles agem como seu próprio banco. Se um usuário perder sua chave privada, os fundos são efetivamente perdidos e não há nada que ele possa fazer a respeito.
- Ineficiência: As *Blockchains* que usam o algoritmo de consenso PoW são altamente ineficientes. Como a mineração é extremamente competitiva e há apenas um vencedor a cada dez minutos, o trabalho de todos os outros mineradores é desperdiçado. Como eles estão sempre tentando aumentar seu poder computacional, para ter uma chance maior de encontrar um *hash* de bloco válido, os recursos usados pela rede aumentaram significativamente nos últimos anos e atualmente consomem mais energia do que muitos países, como a Dinamarca, a Irlanda e a Nigéria.
- Armazenamento: Os livros das *Blockchains* podem crescer muito ao longo do tempo. A Blockchain do Bitcoin atualmente requer cerca de 200 GB de armazenamento. A velocidade no crescimento das *Blockchains* parece estar superando o visto na capacidade dos discos rígidos (HDs) e a rede corre o risco de perder nodes se o livro ficar muito grande, impedindo que usuários baixem e armazenem o mesmo.

3.2 Criptomoedas

O surgimento da criptomoeda foi iniciado pelo misterioso Satoshi Nakamoto, cuja identidade é desconhecida. Ele é o criador do Bitcoin, a criptomoeda mais conhecida e utilizada atualmente. A inovação do Bitcoin é que ele permite transações diretamente entre as pessoas (peer-to-peer), sem a necessidade de confiar em instituições financeiras ou em bancos centrais. Além disso, o Bitcoin é difícil de ser rastreado, o que garante a privacidade dos usuários.

Antes do Bitcoin, já haviam sido criadas outras criptomoedas, como o ecash, desenvolvido por David Chaum em 1983, e o digicash, de 1995. No entanto, foi a partir de 2009, com o desenvolvimento de novas tecnologias, que surgiram muitas outras criptomoedas baseadas no blockchain, que é a principal fonte de funcionamento dessas moedas.

> Considerando o atual arranjo monetário de moedas fiduciárias de papel, a maior parte da massa monetária é constituída de meros dígitos eletrônicos no ciberespaço, dígitos estes criados, controlados e monitorados pelo vasto sistema bancário sob a supervisão de um banco central. Dinheiro material ou físico é utilizado apenas em pequenas compras do dia a dia. O cerne do nosso sistema monetário já é digital e intangível. (ULRICH 2014, p. 63)

Atualmente, é impossível saber exatamente quantas criptomoedas existem no

mercado, devido à facilidade de criação e à crescente demanda por parte de empresas e investidores.

As criptomoedas são moedas digitais que não são controladas por nenhum governo, órgão ou instituição financeira. O principal objetivo de sua criação é facilitar as transações em blockchain, ou seja, transferências diretas entre as pessoas sem a necessidade de um banco intermediário. Com o uso crescente dessas moedas, elas passaram a ser utilizadas como meio de troca entre as pessoas, permitindo a compra de produtos e serviços com moeda digital. Além disso, elas também podem ser usadas como investimento, com o potencial de gerar lucros com o aumento do valor da moeda no mercado financeiro.

O blockchain é a base para o funcionamento das criptomoedas, pois é nele que são armazenadas todas as informações sobre as transações realizadas com essas moedas. Além disso, o blockchain também serve como um livro-razão público, impedindo que qualquer pessoa altere ou exclua dados sem a autorização do dono. Cada criptomoeda tem um valor particular e é possível converter essas moedas em outras moedas digitais, exceto em moedas físicas como o dólar ou o real.

4. Protótipo

Aplicando os conceitos definidos no artigo até o presente momento, foi desenvolvido um protótipo de aplicação para emularmos o funcionamento da utilização de uma blockchain em um sistema eleitoral.

4.1. Metodologia

Foi utilizado para esse desenvolvimento as seguintes ferramentas:

- Linguagem: *Javascript*, com os seguintes *packges*: "*node-forge*", "*node-cache*" e "*crypto-js*";
- Ambiente: *node.js*;
- *IDE*: *Visual Studio Code*.

4.2. Desenvolvimento

Iniciou-se o protótipo com o desenvolvimento da menor parte de um blockchain: seus blocos. Na escrita do código criamos uma classe de nome "*Block*" com os seguintes dados:

- "*Index*": Número de Ordem do bloco.
- "*TimeStamp*", Carimbo de Data da criação do bloco.
- "*Data*": Informações contidas no bloco, em nosso caso o CPF e o Voto do usuário.
- "*PreviousHash*": *Hash* do bloco antecessor.
- "*Hash*": *Hash* criptográfica de todos dados do bloco.
- "*Nonce*": Número de interações para atingir o resultado da dificuldade.

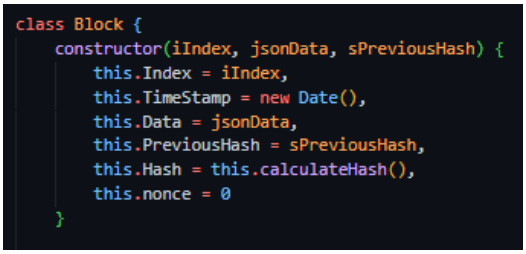

Figura 4. Código do Bloco

Fonte: Autor

Adicionou-se então o método "CalculeHash" que com a biblioteca "*Cripto-Js*" nos retorna o resultado criptografado no bloco pelo algoritmo *SHA256*.

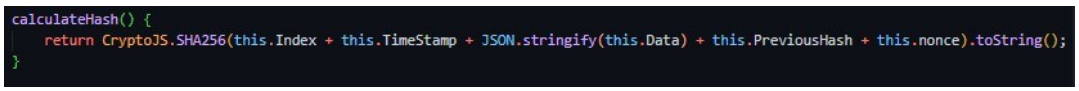

Figura 5. Método para calcular *SHA256*

Fonte: Autor

Criado o código base de um bloco torna-se necessário então criar o código base de uma corrente para isso criamos uma classe nomeada "*Chain*" com as seguintes propriedades:

- "*Zone*": Número da zona eleitoral.
- "*Section*", Número da Seção eleitoral.
- "*Blocks*": *Array* para armazenar os blocos da corrente.
- "*Difficulty*": Dificuldade para minerar a *hash* de um bloco.
- "*isChainValid*": *Boolean* para verificarmos se a corrente está válida, ou seja, não foi alterada ou manipulada.

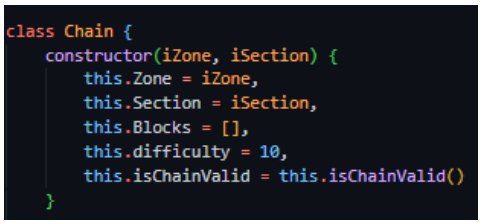

Figura 6. Código da Corrente

Fonte: Autor

Para garantirmos que a corrente esta valida e não foi adulterada iteramos por todos os blocos recalculando a hash e a comparando com a atual, realizando o mesmo processo para a Hash do bloco anterior, assim temos uma camada de segurança que caso ocorra alguma alteração em algum bloco o invasor deve recalcular a hash de toda a cadeia.

```
isChainValid() {
    for (let i = 1; i < this.Blocks.length; i++) {
        const oCurrentBlock = this.Blocks[i];
        const oPreviousBlock = this.Blocks[i - 1];
        if (oCurrentBlock.Hash !== oCurrentBlock.calculateHash()) {
            return false;
        }
        if (oCurrentBlock.PreviousHash !== oPreviousBlock.Hash) {
            return false;

        }
    }
    return true;
}
```

Figura 7. Método para checar a corrente

Fonte: Autor

Pode-se também controlar a dificuldade para calcular a *hash* da *blockchain*, para isso criamos uma função que forca o cálculo da *SHA256* até ela atingir uma condição especificada em nosso caso a quantidade de zeros na *hash*.

```
mineBlock(iDifficulty) {
    while (this.Hash.substring(0, iDifficulty) !== Array(iDifficulty + 1).join("0")) {
        this.nonce++;
        this.Hash = this.calculateHash();
    }
}
```

Figura 8. Método para calcular *Hash* do bloco

Fonte: Autor

4.3 Resultados

Inserindo um bloco em nosso protótipo criado obtivemos a seguinte cadeia de dificuldade três que reflete no começo da *hash* do bloco gênesis.

```
Zone: '230',
Section: '0230',
Blocks: [
  Block {
    Index: 0,
    TimeStamp: 2022-11-03T22:35:17.559Z,
    Data: [Object],
    PreviousHash: '0',
    Hash: '000ee3da7e7529e14cc157400afdca567bcacf5e66bcd4866f92a74430688f2a',
    nonce: 6757
  }
],
difficulty: 3,
isChainValid: true
```

Figura 9. Exemplo da corrente

Fonte: Autor

Adicionando outros blocos conseguimos o seguinte resultado onde é criado um bloco de index um, onde temos a hash do bloco gênesis como *PreviousHash*.

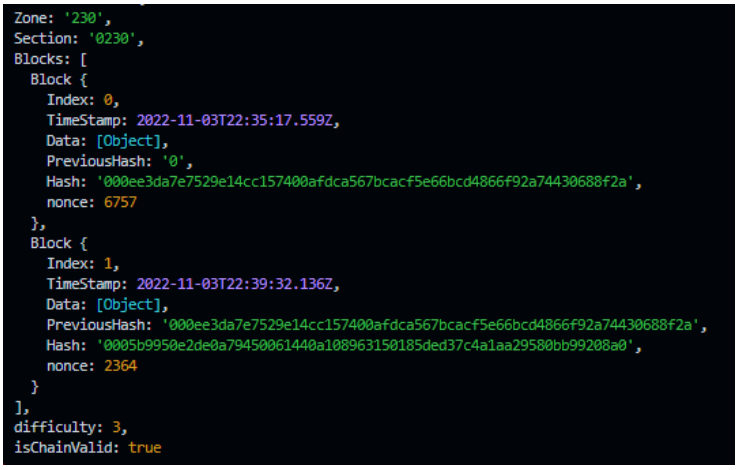

Figura 10. Segundo exemplo da corrente

Fonte: Autor

Caso algum dos blocos sofresse alguma alteração precisaríamos recalcular todas as hashs de todos os blocos para obtermos uma corrente válida pois as hashs dos blocos não estariam de acordo com seus valores originais, quanto maior a dificuldade para minerar um bloco maior o tempo necessário para calcularmos sua hash. Um bloco na dificuldade três leva em torno de 985 *milliseconds* para se calculado e 2939 interações.

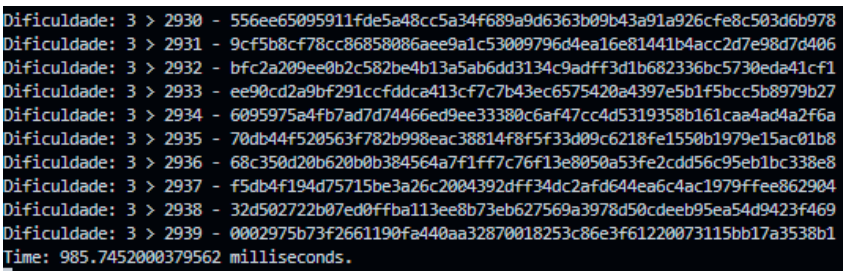

Figura 11. Exemplo do cálculo da *hash*

Fonte: Autor

Enquanto um bloco de dificuldade quatro leva em torno de 2130 *milliseconds* e 8917 interações, logo torna-se inviável para um atacante recalcular centenas de blocos para validar uma corrente não válida.

Figura 12. Segundo exemplo do cálculo da *hash*

Fonte: Autor

5 Considerações Finais

Com base nas informações pesquisadas e apresentadas para o desenvolvimento deste artigo pode-se compreender os benefícios e contras da utilização da tecnologia *blockchain* e o motivo por traz de sua popularidade nos tempos atuais e a sua utilização em um sistema de votação.

Com a utilização de algoritmos de *hashs* criptográficas seguras torna-se uma tarefa extremamente dificultosa para qualquer invasor que tentar realizar qualquer tipo de ataque de alteração na *blockchain* devido o mesmo ter que recalcular as *hashs* de todos os blocos da cadeia levando em conta que o período necessário para realizar esta quebra de uma *hash* em casos pode demorar anos.

Somando ao uso de uma rede descentralizada e a distribuição dos nós para múltiplas autoridades públicas confiáveis de partidos diferentes caso algum atacante consiga quebrar as *hashs* de uma corrente o mesmo deve para tornar os dados alterados validos obter o controle de cinquenta e um porcento de todas as cadeias e alterar suas *hashs*.

No caso da votação dos eleitores, existem-se múltiplas formas de se aplicar este ponto como a utilização de *facecheck* em celulares, urnas como as já existentes atualmente ou a distribuição de chaves privadas a população.

Cria-se assim uma rede de baixo custo e extremamente segura em que se pode realizar auditorias com facilidade assim resolvendo questões como a desconfiança e atende os requisitos dos pilares de segurança da informação como integridade, confiabilidade e disponibilidade.

Essas características tornam a tecnologia blockchain uma opção atraente para aplicações como sistemas de votação.

A popularidade da tecnologia blockchain tem crescido nos últimos anos devido a sua eficiência e segurança. É uma alternativa confiável e segura para aplicações que necessitam de um sistema de banco de dados distribuído, como sistemas de votação. Ao mesmo tempo, é importante ressaltar que a tecnologia ainda está em desenvolvimento e precisa ser aprimorada em vários aspectos.

Referências

PEIXOTO, Mário C. P. Engenharia social e segurança da informação na gestão corporativa. São Paulo: Brasport, 2006.

MITINICK, *The Art of Deception*. São Paulo: Brasport, 2003.

SANTOS, Cleorbete; PRATA, David Nadler; ARAUJO, Humberto Xavier. Fundamentos da Tecnologia Blockchain. 2019. E-book.

MENDES, A. J. B.; PAULICENA, E. H.; SOUZA, W. A. R. Criptografia Quântica: Uma Abordagem Direta. Revista de Sistemas de Informação da FSMA, v. 71

ACADEMY, Binance. Vantagens e Desvantagens da Blockchain. Disponível em: <https://academy.binance.com/pt/articles/positives-and-negatives-of-blockchain>. Acesso em: 14 nov. 2022.

ULRICH, Fernando. Bitcoin: a moeda na era digital. 1. ed. São Paulo: Instituto Ludwig Von Mises Brasil, 2014.