FACULDADE DE TECNOLOGIA DE AMERICANA "Ministro Ralph Biasi"
Curso Superior de Tecnologia em Segurança da Informação

Ana Carolina Martins Feitosa

Vinícius Takasuca Costa

MANUTENÇÃO DA INTEGRIDADE DE EVIDÊNCIAS DIGITAIS UTILIZANDO A *BLOCKCHAIN*

Americana, SP

2025

FACULDADE DE TECNOLOGIA DE AMERICANA "Ministro Ralph Biasi"
Curso Superior de Tecnologia em Segurança da Informação

Ana Carolina Martins Feitosa

Vinícius Takasuca Costa

MANUTENÇÃO DA INTEGRIDADE DE EVIDÊNCIAS DIGITAIS UTILIZANDO A *BLOCKCHAIN*

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação sob a orientação do Prof. Dr. Henri Alves de Godoy.

Área de concentração: Segurança da informação.

Americana, SP

2025

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana Ministro Ralph Biasi- CEETEPS
Dados Internacionais de Catalogação-na-fonte

FEITOSA, Ana Carolina Martins

Manutenção da integridade de evidências digitais utilizando a blockchain. / Ana Carolina Martins FEITOSA, Vinícius Takasuca COSTA – Americana, 2025.

36f.

Monografia (Curso Superior de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana Ministro Ralph Biasi – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Prof. Dr. Henri Alves de GODOY

1. Armazenamento de dados 2. Criptografia 3. Documentos digitais. I. FEITOSA, Ana Carolina Martins, II. COSTA, Vinícius Takasuca III. GODOY, Henri Alves de IV. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana Ministro Ralph Biasi

CDU: 681.3.05
681.518.5
930025

Elaborada pelo autor por meio de sistema automático gerador de ficha catalográfica da Fatec de Americana Ministro Ralph Biasi.

Ana Carolina Martins Feitosa

Vinícius Takasuca Costa

Manutenção da integridade de evidências digitais utilizando a blockchain

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 Ministro Ralph Biasi.
Área de concentração: Segurança da informação.

Americana, 02 de dezembro de 2025.

Banca Examinadora:

Henri Alves de Godoy
Doutor
Fatec Americana "Ministro Ralph Biasi"

Edson Roberto Gaseta
Mestre
Fatec Americana "Ministro Ralph Biasi"

Eduardo Antonio Vicentini
Mestre
Fatec Americana "Ministro Ralph Biasi"

RESUMO

O aumento no volume de dados digitais trouxe consigo o crescimento expressivo das evidências digitais utilizadas em investigações e auditorias, intensificando a necessidade de garantir sua integridade e segurança, evitando adulterações e falhas na cadeia de custódia. Como alternativa para mitigar essas vulnerabilidades, destaca-se a tecnologia *blockchain*, que consiste em um registro imutável, com dados organizados em blocos criptograficamente encadeados e distribuídos de forma descentralizada. Manter a integridade da cadeia de custódia é fundamental para assegurar a autenticidade das evidências digitais desde sua coleta até a apresentação como prova, sendo que qualquer comprometimento nesse processo pode invalidá-las. A problemática abordada neste trabalho são os impactos da quebra da integridade das evidências digitais. O objetivo da pesquisa é analisar como a tecnologia *blockchain* pode ser aplicada para garantir a integridade e autenticidade das evidências digitais. O estudo adota uma abordagem qualitativa, de caráter exploratório, fundamentado em pesquisa bibliográfica, além de incluir uma demonstração prática por meio da rede de testes Ethereum Sepolia.

Palavras-chave: armazenamento de dados, criptografia, documentos digitais.

ABSTRACT

The increasing volume of digital data has led to a significant rise in digital evidence used in investigations and audits, highlighting the need to ensure its integrity and security by preventing tampering and failures in the chain of custody. As an alternative to address these vulnerabilities, blockchain technology stands out, functioning as an immutable record with data organized in cryptographically linked blocks and distributed in a decentralized manner. Maintaining the integrity of the chain of custody is essential to ensure the authenticity of digital evidence from its collection to its presentation in legal proceedings, as any compromise may invalidate it. This study addresses the impacts of the breach of integrity in digital evidence. The objective is to analyze how blockchain technology can be applied to ensure the integrity and authenticity of digital evidence. The study adopts a qualitative, exploratory approach based on bibliographic research, and also a practical demonstration using the Ethereum Sepolia test network.

Keywords: *data storage, cryptography, digital documents.*

LISTA DE ILUSTRAÇÕES

Figura 1 - Representação das informações contidas em um bloco 14
Figura 2 - Exemplificação da vinculação entre blocos por meio do hash 14
Figura 3 - Fluxograma do desenvolvimento do protótipo 22
Figura 4 – Interface do Remix IDE 22
Figura 5 – Redes de teste na MetaMask 24
Figura 6 - Google Cloud Web3 24
Figura 7 – Aba Deploy & Run Transactions no Remix IDE 25
Figura 8 – Confirmação na MetaMask para publicação do contrato inteligente 26
Figura 9 – Geração do hash no Windows 27
Figura 10 – Inserindo o hash no Remix IDE 27
Figura 11 – Transação para registro do hash 28
Figura 12 – Página inicial do Etherscan 29
Figura 13 – Histórico de transações do endereço utilizado no projeto 29
Figura 14 – Página de detalhes da transação 30
Figura 15 – Consulta de evidências registradas 31

LISTA DE ALGORITMOS

Algoritmo 1 – Algoritmo para registro de hash.....23

LISTA DE ABREVIATURAS E SIGLAS

EVM: Ethereum *Virtual Machine*

IDE: *Integrated Development Environment*

PoS: *Proof-of-Stake.*

PoW: *Proof-of-Work.*

SUMÁRIO

INTRODUÇÃO **11**
1. FUNDAMENTAÇÃO TEÓRICA **13**
1.1. Blockchain **13**
1.2. Hash **15**
1.3. Nonce e Dificuldade **15**
1.4. Consenso, Proof-of-Work e Proof-of-Stake **16**
1.5. Perícia Forense Digital **17**
1.6. Evidências Digitais **17**
1.7. Cadeia de Custódia **17**
1.8. Integridade **17**
1.9. Ethereum e Ethereum Sepolia Testnet **18**
1.10. Contratos inteligentes **18**
1.11. RemixIDE, Solidity e MetaMask **18**
2. METODOLOGIA **20**
2.1. Caracterização de Pesquisa **20**
2.2. Quanto ao delineamento **20**
3. DESENVOLVIMENTO **21**
4. CONSIDERAÇÕES FINAIS **32**
REFERÊNCIAS **34**

INTRODUÇÃO

A evolução tecnológica das últimas décadas resultou em um aumento significativo no volume de dados gerados e das transmissões de informações por meio digital. Entre eles pode-se destacar as evidências digitais que cresceram exponencialmente com a popularização da internet e são usadas em processos judiciais, investigações e auditorias, exigindo sistemas cada vez mais seguros que possam garantir sua integridade e confidencialidade em um contexto onde invasões, acessos não autorizados, falhas na cadeia de custódia e adulterações são possíveis.

Dessa forma, a tecnologia de *blockchain* se destaca como uma alternativa oportuna para combater essas vulnerabilidades. A *blockchain* é um registro imutável que contém dados estruturados em blocos criptograficamente encadeados entre si e de forma descentralizada. Sua aplicação no mercado financeiro é uma demonstração de sua capacidade, que é também de onde seu conceito surgiu: da procura de um modo alternativo de assegurar a credibilidade e processamento de pagamentos em transações financeiras sem necessitar de terceiros, sendo implementada à moeda Bitcoin (NAKAMOTO, 2008).

A integridade de uma cadeia de custódia, que é o instrumento que garante a autenticidade da evidência digital desde sua coleta até sua apresentação como prova, é vital, visto que qualquer comprometimento em seu processo o torna inválido. Essa é a problemática abordada no presente trabalho, levantada da questão “qual o impacto da quebra de integridade de evidências digitais na cadeia de custódia em uma investigação forense?”.

Assim, a importância do trabalho reside na contribuição para o debate sobre segurança da informação em ambientes digitais, propondo soluções modernas para desafios antigos, como a preservação da autenticidade de provas eletrônicas. Com a proliferação de crimes cibernéticos e fraudes digitais, explorar o potencial da *blockchain* para fortalecer a confiança em processos jurídicos e administrativos é essencial para modernizar práticas e garantir maior segurança dos dados.

O trabalho é viável pois possui uma considerável disponibilidade de literatura técnica e científica atualizada sobre *blockchain* e sua aplicação em segurança da informação. O crescente interesse de setores jurídicos e tecnológicos no tema também é um fator que reforça a relevância e aplicabilidade da pesquisa.

O objetivo do trabalho é analisar como a tecnologia *blockchain* pode ser aplicada para garantir a integridade e autenticidade de evidências digitais. Como

objetivos específicos temos: compreender os princípios básicos de *blockchain*, investigar os métodos de preservação e suas vulnerabilidades, identificar os benefícios e o futuro da aplicação dessa tecnologia.

Este estudo tem como percurso metodológico uma abordagem qualitativa de caráter exploratório, baseando-se na pesquisa bibliográfica, com levantamento e análise de livros, artigos científicos, relatórios técnicos, legislações e fontes online confiáveis relacionados à *blockchain*, segurança da informação, cadeia de custódia digital e perícia forense. Como complemento, foi desenvolvido um protótipo para aplicação real em uma rede *blockchain*, de forma a comprovar a funcionalidade da tecnologia e seu uso para garantir a imutabilidade e integridade de evidências digitais.

O trabalho está organizado em três capítulos, sendo o capítulo I a fundamentação teórica, o capítulo II apresenta o percurso metodológico, o capítulo III conterá o desenvolvimento do protótipo para aplicação real, e o capítulo IV conterá os resultados, análise e discussão dos dados.

1. FUNDAMENTAÇÃO TEÓRICA

1.1. Blockchain

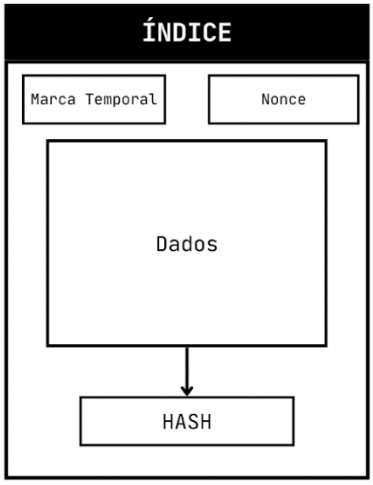
Visando uma alternativa a necessidade de terceiros de confiança para segurança e processamento de pagamentos eletrônicos no comércio por meio da internet, como instituições financeiras ou cartórios, o conceito que ficou conhecido como *blockchain* foi introduzido em 2008 por Satoshi Nakamoto (pseudônimo) no artigo "*Bitcoin: A Peer-to-Peer Electronic Cash System*" (NAKAMOTO, 2008). A proposta era um mecanismo que garantisse a imutabilidade sem a necessidade de terceiros por meio de uma rede totalmente "*peer-to-peer*", formando um consenso entre participantes não confiáveis que mantém os registros de forma descentralizada. Para garantir a confiabilidade e segurança, as transações possuem um registro com data e hora, organizadas de forma sequencial em blocos encadeados, onde cada novo bloco depende criptograficamente do anterior, criando um histórico imutável. (NAKAMOTO, 2008).

Inicialmente implementada para transações com a moeda Bitcoin, a tecnologia de *blockchain* pode ser encontrada em vários contextos como controle de transações, votos eletrônicos, Internet das Coisas, registro de dados de saúde, entre outros (LUNARDI et al., 2024). É definido como “uma estrutura de dados compartilhada que permite o armazenamento de transações de forma digital e descentralizada, sem a necessidade de uma autoridade central” (SOUZA, 2024). Essas transações são armazenadas em um registro, também conhecido como livro razão, distribuído entre todos os usuários que estão na rede e que podem ser usados para verificar qualquer alteração.

Os dados dessas transações são agregados em blocos replicados na rede, com informações de data e hora, criptografados e diretamente ligados ao bloco anterior (ANDONI et al., 2019), o que forma uma cadeia de blocos que origina o nome da tecnologia. Devido a esse vínculo com a formação anterior, as chances de qualquer mudança são improváveis.

Em uma *blockchain* podemos encontrar uma estrutura que se assemelha a uma corrente, com blocos seguindo uma sequência e contendo as seguintes informações, como ilustrado na Figura 1: índice, marca temporal, hash, hash anterior, conteúdo/dado e nonce.

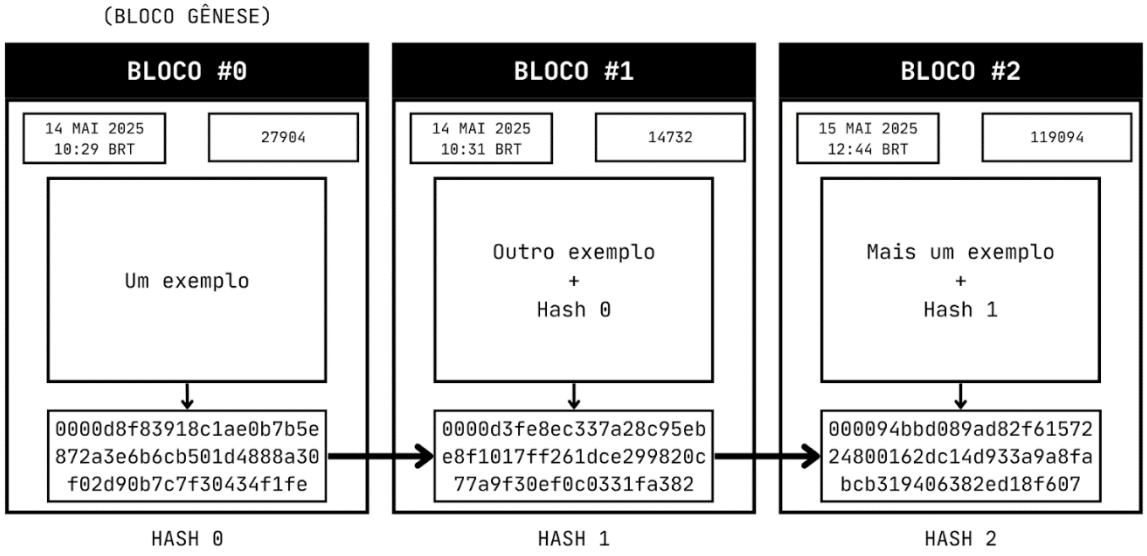
Figura 1 - Representação das informações contidas em um bloco



Fonte: Autoria própria (2025).

O índice indica a posição do bloco na cadeia, com o primeiro bloco da cadeia possuindo o índice 0, também conhecido como bloco gênese. O seguinte, então, teria o índice 1, o próximo teria o índice 2 e assim por diante. Em seguida, encontra-se o marco temporal que registra a data e hora de sua criação, além de ajudar a manter a *blockchain* ordenada. Os dados passarão pelo processo de hashing para gerar uma saída de tamanho fixo e irreversível, a Figura 2 demonstra esse processo:

Figura 2 - Exemplificação da vinculação entre blocos por meio do hash



Fonte: Autoria própria baseada em Souza (2024).

A partir do bloco gênese, que é o primeiro bloco da cadeia, todos os outros estão vinculados ao anterior por meio de criptografia e uso do algoritmo de hash.

Devido a sua natureza, cria-se uma espécie de impressão digital, de forma que qualquer alteração em um bloco consequentemente cria outro hash e passa invalidar aquele bloco e os seguintes.

Antes de prosseguir com o restante das informações, é importante entender conceitos fundamentais e que se relacionam na tecnologia de *blockchain*: hash, nonce, dificuldade, Prova de Trabalho e Prova de Participação.

1.2. Hash

O hash utilizado na *blockchain* para identificar blocos é resultado de uma função hash criptográfica, que gera uma saída de tamanho fixo independente da entrada e é muito utilizado na verificação de integridade de dados. Um exemplo de algoritmo é o SHA-256, parte da família SHA-2, que gera uma saída de 256 bits e é usado no bitcoin para validação de blocos e Prova de Trabalho. O NIST (2025) lista 3 características que uma função hash deve apresentar para ser aprovada:

- Resistência à Colisão: significa que é computacionalmente inviável encontrar duas entradas diferentes que gerem o mesmo hash.
- Resistência à Pré-Imagem: a partir de um hash, é computacionalmente inviável encontrar uma entrada que gere esse mesmo valor de hash.
- Resistência à Segunda Pré-Imagem: é computacionalmente inviável encontrar uma segunda entrada que tem o mesmo valor de hash.

Assim, o hash garante que os dados registrados permaneçam íntegros e inalterados, pois qualquer modificação no conteúdo altera completamente o valor gerado, comprometendo a validade não só do bloco, mas da cadeia como um todo. Segundo Miranda e Zuchi (2018) "o hash é uma assinatura digital de um bloco, esta é usada para encadeá-lo ao bloco anterior, e este ligado ao seu bloco antecessor e assim por diante até o primeiro bloco desta cadeia".

1.3. Nonce e Dificuldade

Nonce, segundo o Dicionário Merriam-Webster, significa "para um único propósito". É um número que modifica o hash até que ele atenda a regra de dificuldade, sendo iterado até que a saída esteja de acordo com esse requisito. Por exemplo, se a dificuldade for definida como 1 bit o hash deve iniciar com um zero, 2 bits exigiriam dois zeros e assim por diante de forma que ao aumentar a dificuldade,

consequentemente, o poder computacional necessário será maior. Essa colisão parcial é fruto do nonce (CHICARINO, V. R. et al., 2017).

1.4. Consenso, Proof-of-Work e Proof-of-Stake

O consenso em uma rede *blockchain* é o processo em que os próprios nós da rede colaboram para validar qual conjunto de blocos deve ser considerado legítimo, visto que não existe uma autoridade central responsável pelas transações. De acordo com Zhang, Xue e Liu (2019), o consenso é essencial para manter a integridade do sistema e garantir que todas as cópias do livro-razão permaneçam sincronizadas entre os nós da rede. Esse processo envolve a definição de qual nó será responsável pela criação do próximo bloco, o que é determinado por meio da implementação de um protocolo de consenso. Quando um nó recebe um novo bloco, ele o verifica e o propaga para os demais participantes. A partir dessas trocas de informações, as cadeias são comparadas e, quando apresentam o mesmo estado, considera-se que a rede atingiu o consenso (CHICARINO et al., 2017). De acordo com Yaga et al. (2018), uma grande parte da motivação para a participação dos nós nesse sistema é financeira, pois eles podem ser recompensados por meio de criptomoedas ou taxas de transação.

A Prova de Trabalho (*Proof of Work*, PoW), utilizada na rede Bitcoin, é um exemplo de protocolo de consenso. Esse mecanismo consiste em resolver um problema computacionalmente exigente, em que sua solução serve como prova de que determinado nó realizou um esforço de processamento. Um método comum é encontrar um número arbitrário, o *nonce*, que gere um *hash* que atenda ao nível de dificuldade imposto pela rede, um processo intensivo devido ao número elevado de tentativas necessárias. Após a validação do bloco pelos demais nós, o minerador é recompensado com criptomoedas (YAGA et al., 2018).

O conceito de PoW foi originalmente proposto por Adam Back (2002) no sistema *Hashcash*, desenvolvido como uma forma de mitigar ataques cibernéticos, como negação de serviço e spam. A ideia é que seja um processo complicado, com uma solução árdua de se encontrar, mas de fácil verificação por meio do hash gerado. A ideia foi utilizada no Bitcoin onde os mineradores gastam uma grande quantidade de energia para encontrar blocos válidos e criar um ambiente descentralizado.

Outro protocolo de consenso notável é a Prova de Participação (*Proof of Stake, PoS*) e, diferente da Prova de Trabalho, não é computacionalmente exigente, levando

em conta a participação para a escolha do criador do próximo bloco. Essa participação, ou *stake*, refere-se a uma quantia de criptomoeda do usuário investida no sistema, bloqueada como garantia. O participante pode receber recompensas pela publicação de blocos válidos, geralmente na forma de taxas de transação pagas pelos próprios usuários (YAGA et al., 2018).

1.5. Perícia Forense Digital

A perícia forense digital é uma área da ciência forense aplicada em contextos como governo, setor privado, instituições financeiras e área jurídica. Sua função é analisar qualquer dispositivo que armazene dados, sendo essencial em investigações de ciberataques e crimes diversos, geralmente com o uso de ferramentas especializadas como o Cellebrite. (HASSAN, 2019)

1.6. Evidências Digitais

Evidências digitais são vestígios deixados na esfera da tecnologia e informática que, assim como vestígios de um crime comum, devem ser isoladas, coletadas e preservadas, formando uma cadeia de custódia. Elas podem ser encontradas em diversos dispositivos, como computadores, celulares, pen drives, câmeras de vídeo ou fotográficas, CDs, e podem assumir várias formas, incluindo imagens, vídeos, músicas, e-mails e sites. (CHAQUIAN FILHO; DUARTE; LACERDA, 2018)

1.7. Cadeia de Custódia

A cadeia de custódia é um instrumento necessário para que evidências digitais tenham validade legal, garantindo a credibilidade da coleta, análise e documentação conforme as técnicas da perícia forense digital, sem irregularidades que possam comprometer a credibilidade do material colhido, possibilitando assim, que posteriormente seja admitido como prova em um processo. (SANTOS; BORGES; RODRIGUES, 2021)

1.8. Integridade

Integridade é o estado ou característica daquilo que permanece intacto. No contexto da informação, refere-se à garantia de que os dados não foram modificados sem autorização, seja de forma intencional ou não. É importante destacar que uma

informação íntegra não necessariamente é uma informação correta, mas sim que não sofreu alterações por interferência interna ou externa. (HINTZBERGEN et al., 2018)

1.9. Ethereum e Ethereum Sepolia Testnet

Ethereum é uma rede *blockchain* descentralizada, pública e aberta, desenvolvida para oferecer funcionalidades como os contratos inteligentes além dos serviços financeiros alimentados através de sua criptomoeda nativa, o Ether (ETH). Com milhares de computadores ao redor do mundo atuando como nós que operam em conjunto para fornecer serviços para qualquer pessoa com conexão à internet, a plataforma oferece vantagens como segurança e confiabilidade. (ETHEREUM FOUNDATION, 2025)

Ethereum Sepolia Testnet é uma rede pública de desenvolvimento e testes de aplicações relacionadas a *blockchain*, como protocolos e contratos inteligentes. Fornece um ambiente semelhante ao da mainnet Ethereum - onde as transações reais são processadas - mas sem o uso de fundos reais, utilizando apenas tokens obtidos por meio de faucets. (SANTOS; PICOLO, 2023)

1.10. Contratos inteligentes

Os contratos inteligentes (*smart contracts*, em inglês) são contêineres de códigos autoexecutáveis com condições previamente definidas entre as partes, que operam em uma infraestrutura descentralizada e são automaticamente verificados através dos nós da rede *blockchain*, dispensando a necessidade de intermediários. (TAHERDOOST, 2023)

São semelhantes aos contratos físicos, à medida que compartilham a necessidade de observância dos princípios contratuais tradicionais do Direito Civil, mas diferenciam-se por funcionarem de maneira totalmente digital, garantindo imutabilidade e transparência entre os participantes. (PORTO; GLÓRIA; FERREIRA, 2022)

1.11. RemixIDE, Solidity e MetaMask

O desenvolvimento e a implantação de contratos inteligentes na rede Ethereum são facilitados pelo ambiente de desenvolvimento integrado (*Integrated Development Environment*, IDE) conhecido como Remix IDE, uma ferramenta baseada em navegador amplamente utilizada para programar e testar contratos escritos em

Solidity, linguagem de programação orientada a objetos e influenciada por linguagens como Python, C++ e JavaScript (ZOTTELE et al., 2023). O código desenvolvido na Remix é executado na Ethereum Virtual Machine (EVM), que processa os contratos inteligentes e garante sua execução em todos os nós da rede (GUIMARÃES, 2024).

Para realizar transações reais ou em redes de teste, utiliza-se a MetaMask, uma extensão de navegador que atua como uma carteira digital, permitindo aos usuários gerenciar seus endereços Ethereum e interagir com aplicações descentralizadas de forma segura. Por meio da MetaMask, é possível conectar a Remix a uma testnet, como a Sepolia, e realizar a publicação e execução de contratos inteligentes (GUIMARÃES, 2024).

2. METODOLOGIA

Este estudo utiliza uma abordagem qualitativa, com caráter exploratória, tendo como método principal a pesquisa bibliográfica para analisar como a tecnologia de *blockchain* pode ser utilizada para proteger evidências digitais. Foram analisados livros, artigos científicos, legislações, relatórios técnicos e materiais online confiáveis relacionados à tecnologia *blockchain*, segurança da informação, cadeia de custódia digital e perícia forense.

O objetivo da metodologia é reunir, interpretar e sintetizar os principais conceitos, aplicações e desafios da utilização da *blockchain* na preservação de evidências digitais. A escolha desse método se justifica pela disponibilidade de material teórico atualizado e pela relevância do tema no contexto atual da transformação digital. Adicionalmente, foi desenvolvida uma demonstração prática envolvendo a criação de um contrato inteligente simples para armazenar hashes de evidências digitais, utilizando a rede de testes Ethereum Sepolia, com o objetivo de avaliar, de maneira aplicada, como o registro de evidências digitais pode ocorrer em um ambiente real de *blockchain*. O uso da rede de testes Ethereum Sepolia se justifica por oferecer um ambiente seguro, público e funcional que mantém as características principais da rede principal como o registro imutável e execução de contratos inteligentes, mas sem custos financeiros por utilizar tokens de testes.

2.1. Caracterização de Pesquisa

Pesquisa de caráter exploratório, de abordagem qualitativa, com foco na compreensão teórica da aplicação da *blockchain* em contextos forenses e de segurança da informação, além de um exemplo real de aplicação.

2.2. Quanto ao delineamento

Trata-se de uma pesquisa bibliográfica, fundamentada em livros, artigos e documentos técnicos atuais que abordam *blockchain*, integridade de dados e cadeia de custódia digital, aliada a uma pesquisa aplicada que inclui a implementação de um protótipo operacional.

3. DESENVOLVIMENTO

Este trabalho desenvolveu uma parte prática com o objetivo de demonstrar o funcionamento da tecnologia *blockchain* na manutenção da integridade de evidências digitais. Para tanto, foi elaborado um protótipo baseado na criação de um contrato inteligente implantado em uma rede de testes, simulando o registro do hash da evidência digital e seu armazenamento na *blockchain*. A proposta é garantir a imutabilidade e verificabilidade dos hashes criptográficos dos arquivos. Dessa forma, realizou-se a simulação da coleta de um arquivo imagem de uma máquina periciada, cujo hash foi gerado localmente. Este valor representa sua impressão digital única e qualquer alteração em seu conteúdo poderá ser facilmente detectada ao comparar os hashes. O foco desta etapa é apresentar uma prova de conceito baseada em tecnologias acessíveis, demonstrando os princípios fundamentais para esse tipo de aplicação.

As ferramentas utilizadas foram a rede de testes da *blockchain* Ethereum, conhecida como Ethereum Sepolia, utilizada para execução e validação de contratos inteligentes sem custos financeiros reais, o Remix IDE, um ambiente de desenvolvimento online para criação, compilação e implantação do contrato inteligente escrito na linguagem de programação solidity, além da carteira MetaMask para gerenciar a conta Ethereum e realizar transações na rede Sepolia.

O processo tem início com a geração do hash do arquivo digital, realizada localmente por uma função criptográfica como o SHA-256, responsável por gerar uma string única correspondente a uma impressão digital. Então, por meio da função *addEvidence()* do contrato inteligente, o hash gerado será enviado à rede Ethereum Sepolia para ser registrado de forma pública e imutável. Assim, para validar a autenticidade do arquivo, basta gerar o hash novamente e comparar com aquele armazenado na *blockchain* e, se coincidirem, quer dizer que o arquivo é íntegro. Todas as etapas estão descritas no fluxograma da Figura 3:

Figura 3 - Fluxograma do desenvolvimento do protótipo

Fonte: Autoria própria (2025).

A preparação do ambiente para a realização da etapa prática contou primeiramente com a criação do projeto no ambiente de desenvolvimento Remix IDE, onde o arquivo para contratos utiliza a extensão ".sol". Com o código escrito em Solidity para o registro dos hashes, o contrato foi então compilado na aba *Solidity Compiler* com a versão 0.8.x, como consta no começo do código e na Figura 4.

Figura 4 – Interface do Remix IDE

Fonte: Autoria própria (2025)

A estrutura do contrato conta com duas funções principais para registro e verificação das evidências, como demonstrado no Algoritmo 1. A função *addEvidence()* realiza a inclusão de um novo hash na *blockchain*, garantindo que o valor informado não esteja vazio e que ainda não tenha sido registrado anteriormente. Já a função *verifyEvidence()* permite consultar se um determinado hash está presente no contrato.

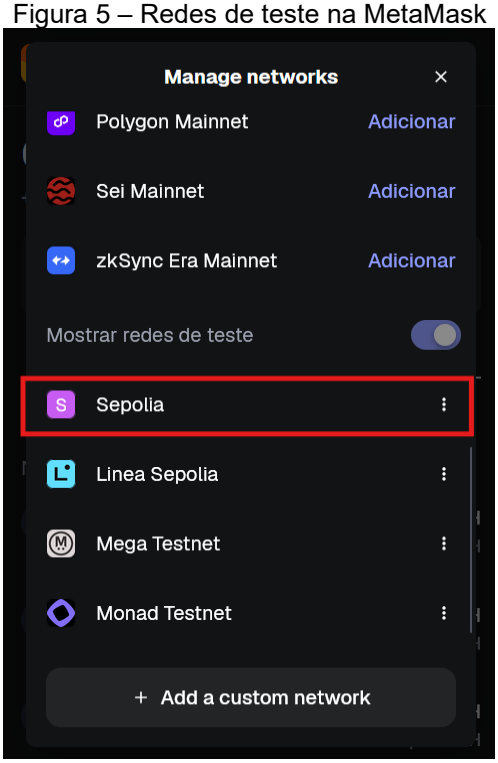
Algoritmo 1 – Algoritmo para registro de hash

```
1  // SPDX-License-Identifier: MIT
2  pragma solidity ^0.8.0;
3
4  contract RegistroEvidencia {
5      struct Evidence {
6          uint256 id;
7          address sender;
8          string fileHash;
9          uint256 timestamp;
10     }
11
12     uint256 public evidenceCount;
13     mapping(uint256 => Evidence) public evidences;
14     mapping(string => bool) public hashExists;
15
16     event EvidenceAdded(uint256 id, address indexed sender, string fileHash,
17       uint256 timestamp);
18
19     function addEvidence(string memory _fileHash) public {
20         require(bytes(_fileHash).length > 0, "Hash vazio.");
21         require(!hashExists[_fileHash], "Este hash ja foi registrado.");
22
23         evidenceCount++;
24         evidences[evidenceCount] = Evidence(evidenceCount, msg.sender,
25 _fileHash, block.timestamp);
26         hashExists[_fileHash] = true;
27
28         emit EvidenceAdded(evidenceCount, msg.sender, _fileHash,
29 block.timestamp);
30     }
31
32     function verifyEvidence(string memory _fileHash) public view returns (bool) {
33         return hashExists[_fileHash];
34     }
35 }
36
```

Fonte: Autoria própria (2025)

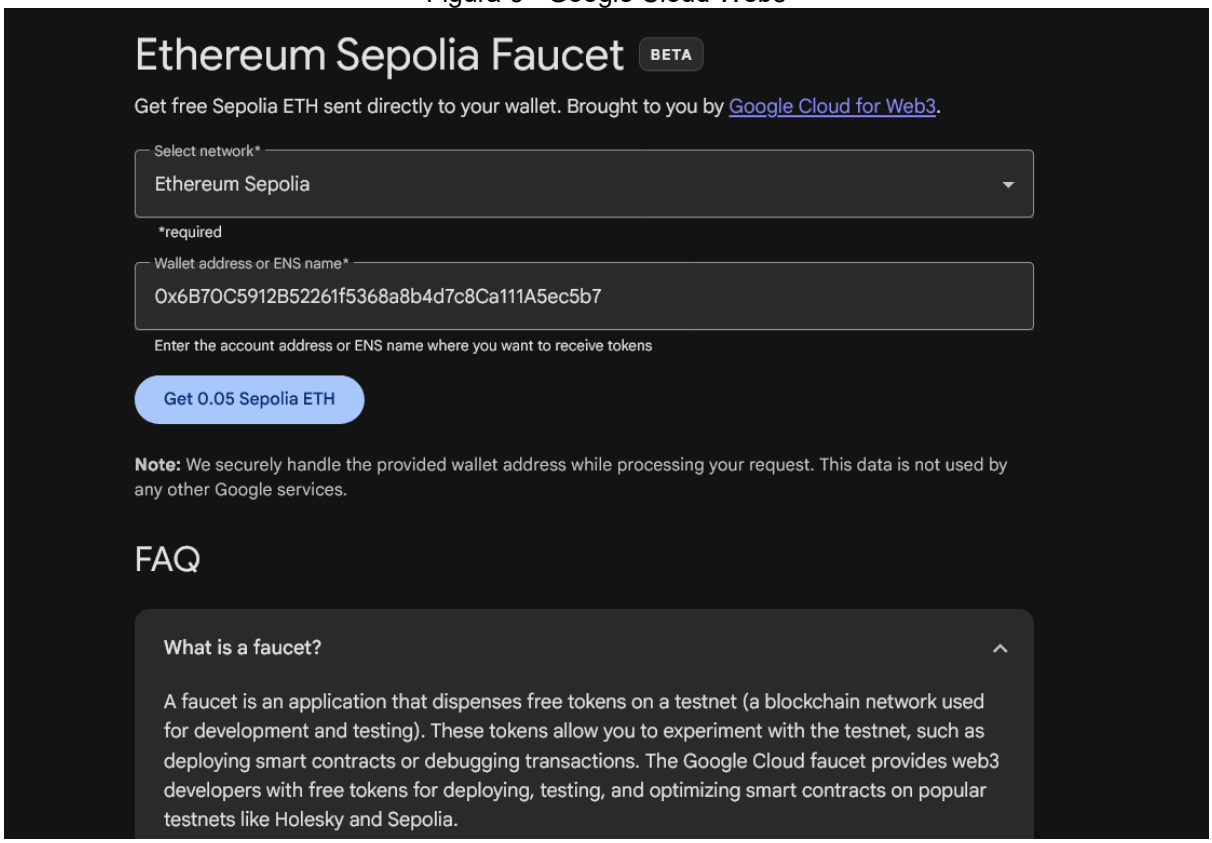
A carteira MetaMask foi utilizada como meio para a publicação e interação com o contrato. Após ser configurada para a testnet Sepolia como mostra a Figura 4, foi necessário adicionar tokens de teste por meio de faucets que são serviços que distribuem pequenas quantidades de criptomoedas de teste, como o Google Cloud Web3 apresentado na Figura 5 e que foi utilizado nesse projeto. Nele é necessário informar o endereço da carteira para o envio dos fundos.

Figura 5 – Redes de teste na MetaMask



Fonte: Autoria própria (2025)

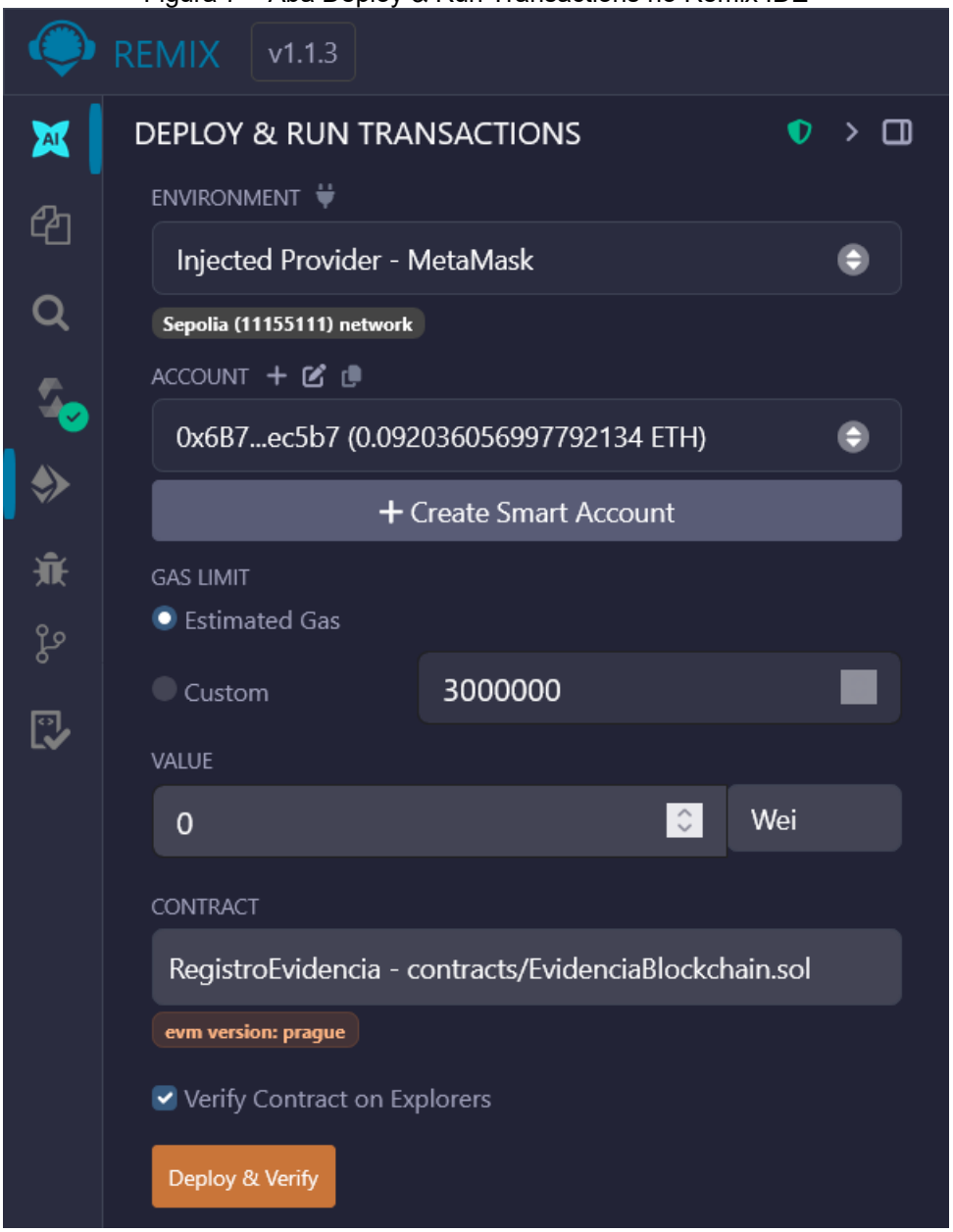
Figura 6 - Google Cloud Web3



Fonte: Autoria própria (2025)

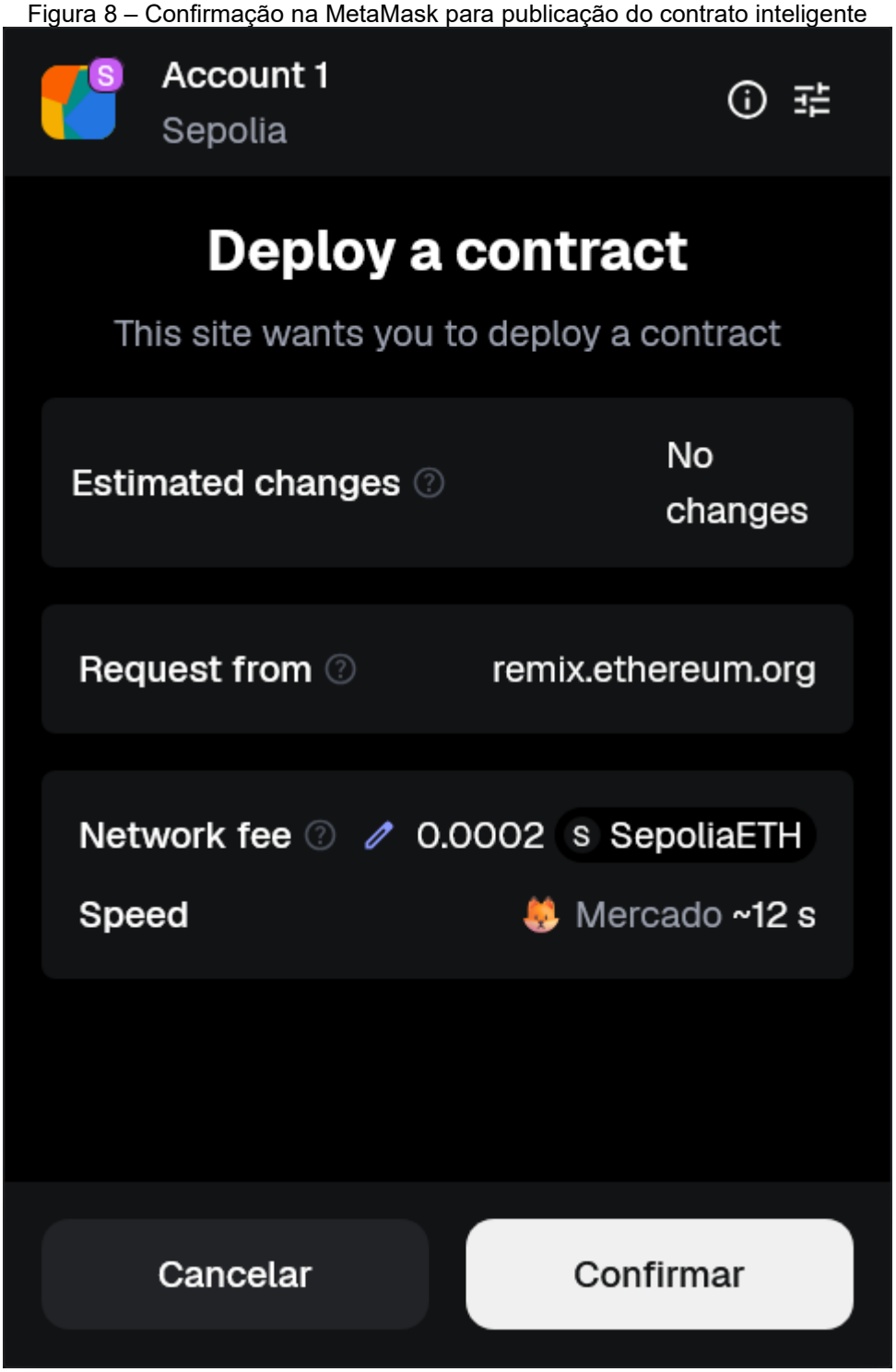
Em seguida, o contrato foi implantado por meio da aba *Deploy & Run Transactions* (Figura 6), selecionando o ambiente "*Injected Provider* – MetaMask", o que conecta o Remix diretamente à carteira configurada na rede Sepolia. Após escolher o contrato na opção *Contract*, uma confirmação será enviada para o MetaMask com uma taxa de transação necessária para que o contrato seja publicado na rede e possa ser testado, conforme observado na Figura 7.

Figura 7 – Aba Deploy & Run Transactions no Remix IDE



Fonte: Autoria própria (2025)

Figura 8 – Confirmação na MetaMask para publicação do contrato inteligente



Fonte: Autoria própria (2025)

Assim que o contrato é implementado, a função *addEvidence()* é utilizada para registrar o hash da evidência digital. Para fins de demonstração, foi simulada a análise de uma imagem forense denominada “imagem.dd”, representando a cópia de uma unidade de armazenamento de uma máquina periciada. Seu hash foi gerada no sistema Windows por meio do comando certutil -hashfile imagem.dd SHA256, como

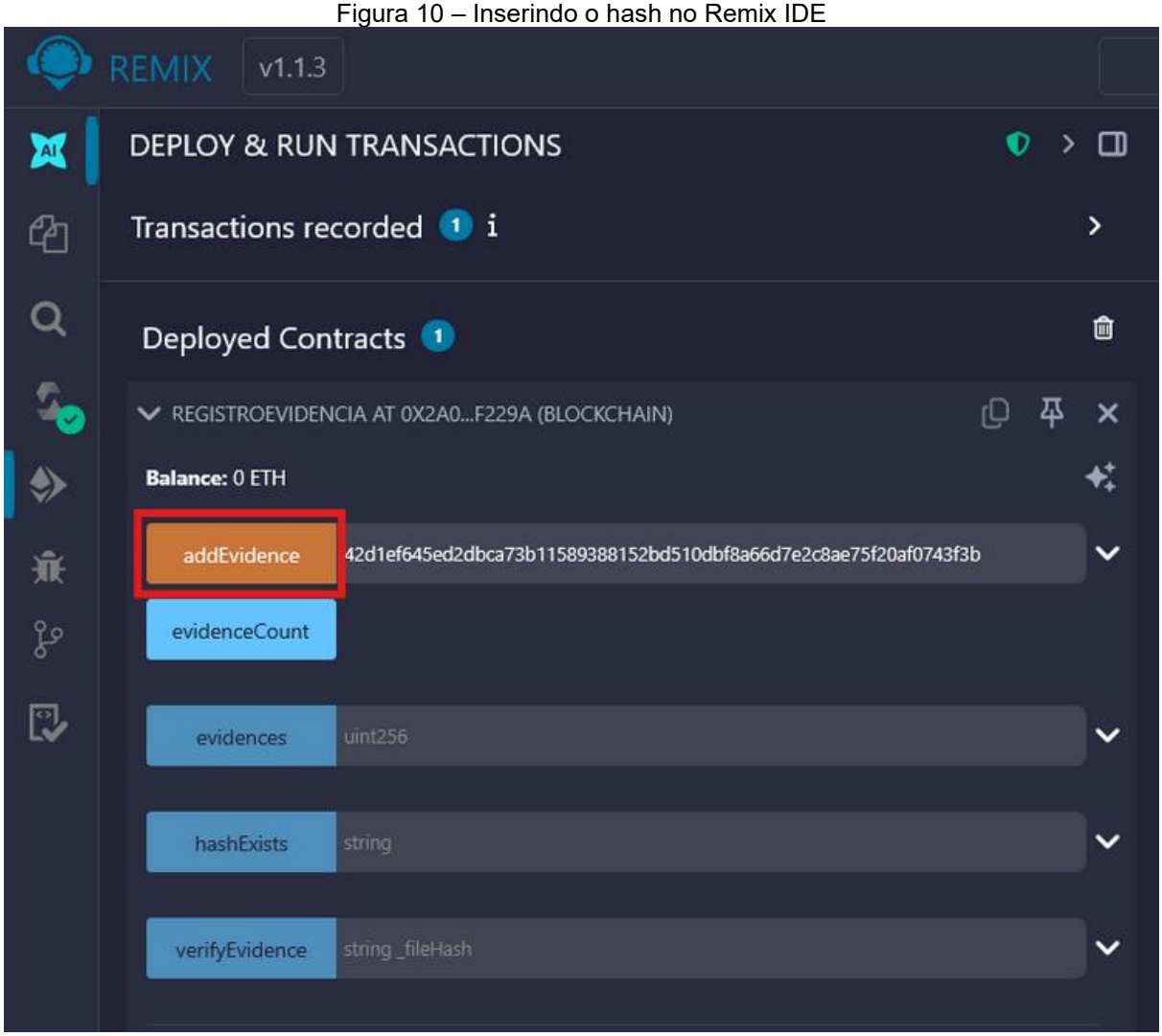
evidenciado na Figura 8. Em seguida, esse valor foi inserido no campo de entrada do Remix IDE (Figura 9), resultando em uma nova transação para que o hash seja registrado na rede Ethereum Sepolia (Figura 10).

Figura 9 – Geração do hash no Windows

```
C:\Users\vini4\Desktop>certutil -hashfile imagem.dd SHA256
SHA256 hash de imagem.dd:
42d1ef645ed2dbca73b11589388152bd510dbf8a66d7e2c8ae75f20af0743f3b
CertUtil: -hashfile : comando concluído com êxito.
```

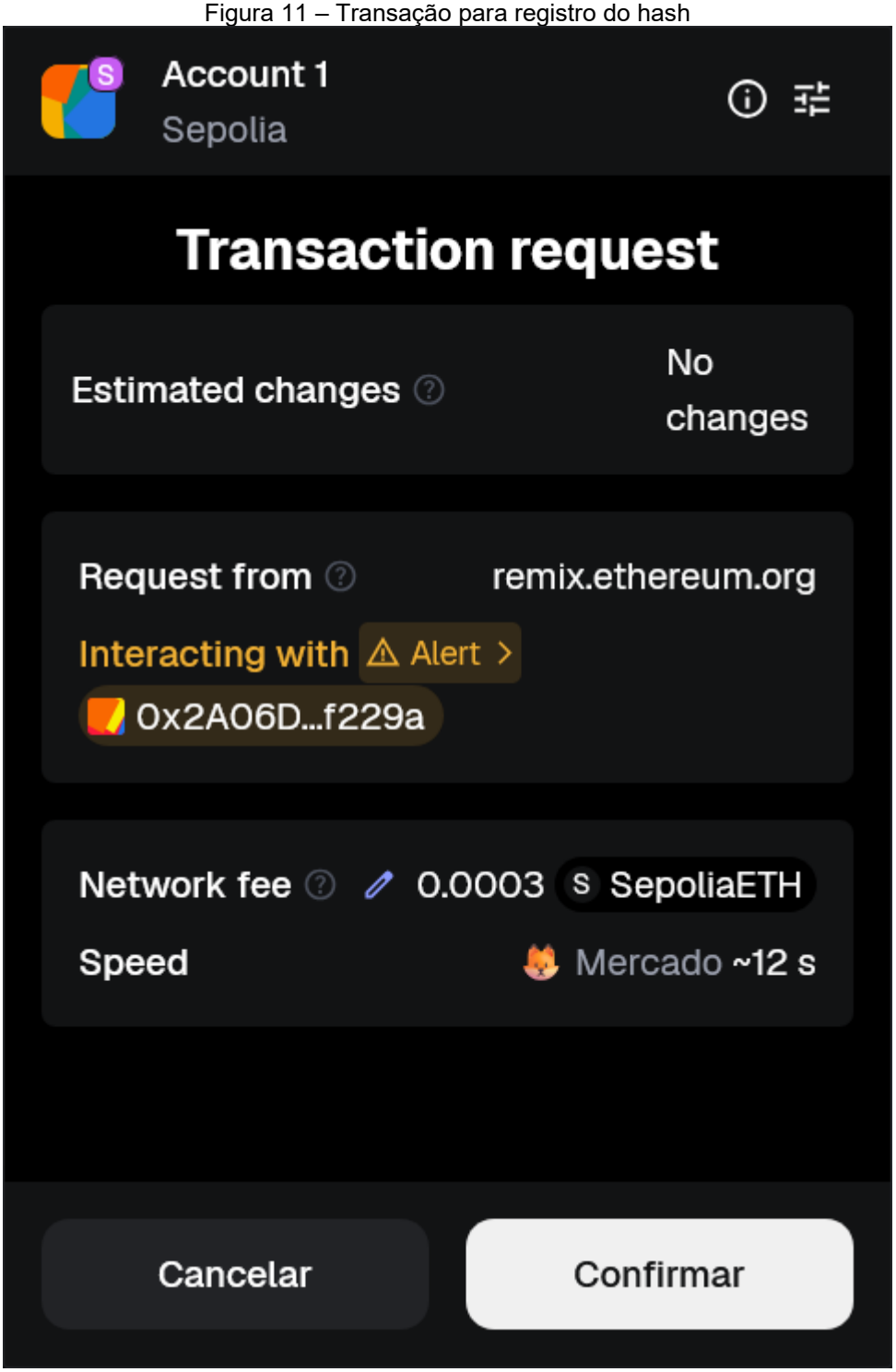
Fonte: Autoria própria (2025)

Figura 10 – Inserindo o hash no Remix IDE



Fonte: Autoria própria (2025)

Figura 11 – Transação para registro do hash

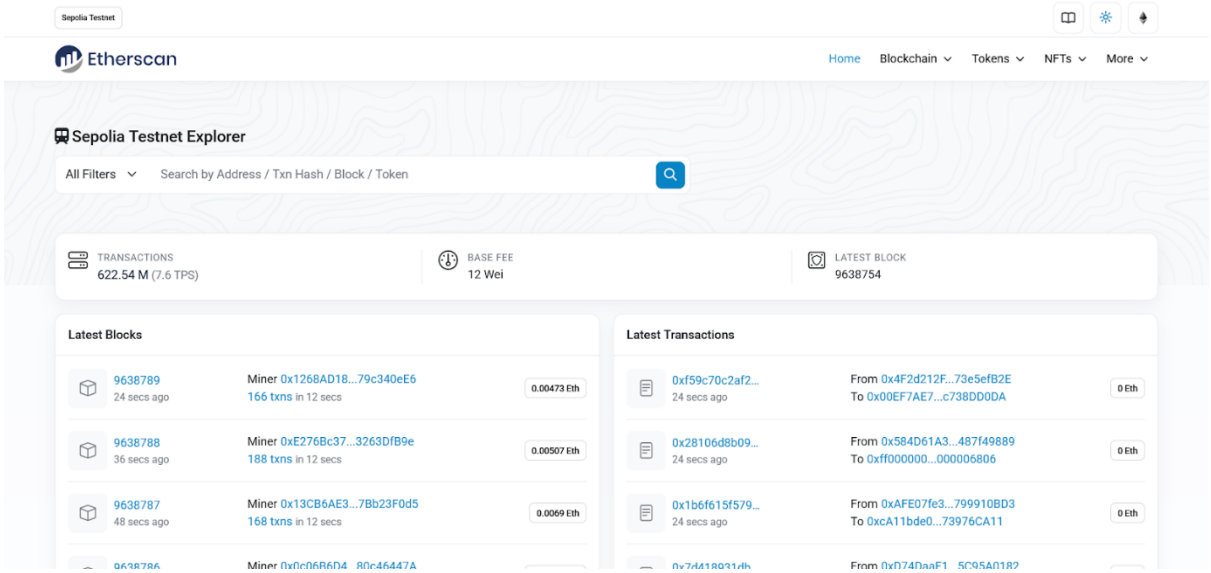


Fonte: Autoria própria (2025)

Após a confirmação, a operação será processada pela rede e os detalhes podem ser vistos no MetaMask, como o consumo de gás e seu status. Uma vez validada, a transação fará parte do histórico da *blockchain*, o que garante a imutabilidade e transparência. Além disso, é possível visualizar informações como o hash da transação, o endereço do remetente, o timestamp e os dados codificados no

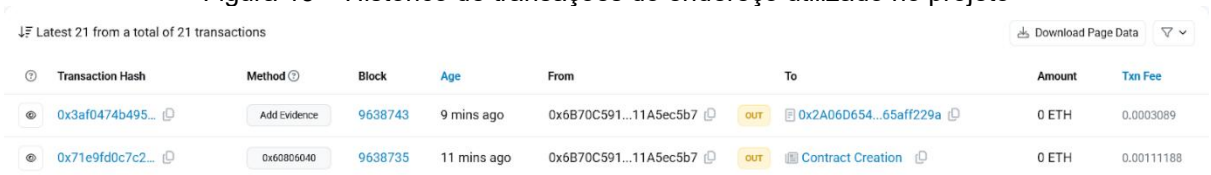
Etherscan, um explorador de blocos onde é possível consultar e verificar transações na rede Ethereum conforme as Figuras de 11 a 13 apresentam.

Figura 12 – Página inicial do Etherscan



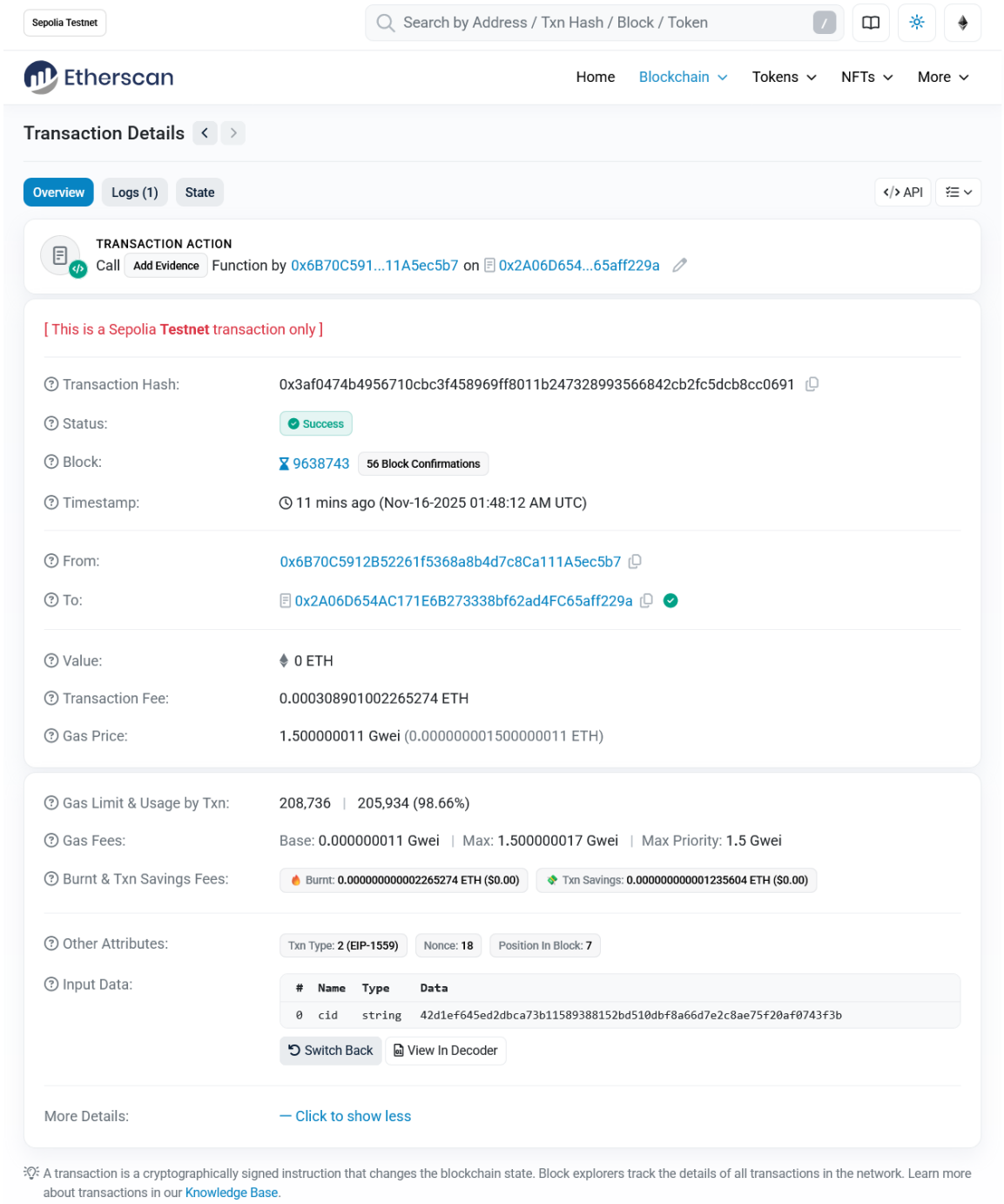
Fonte: Autoria própria (2025)

Figura 13 – Histórico de transações do endereço utilizado no projeto



Fonte: Autoria própria (2025)

Figura 14 – Página de detalhes da transação

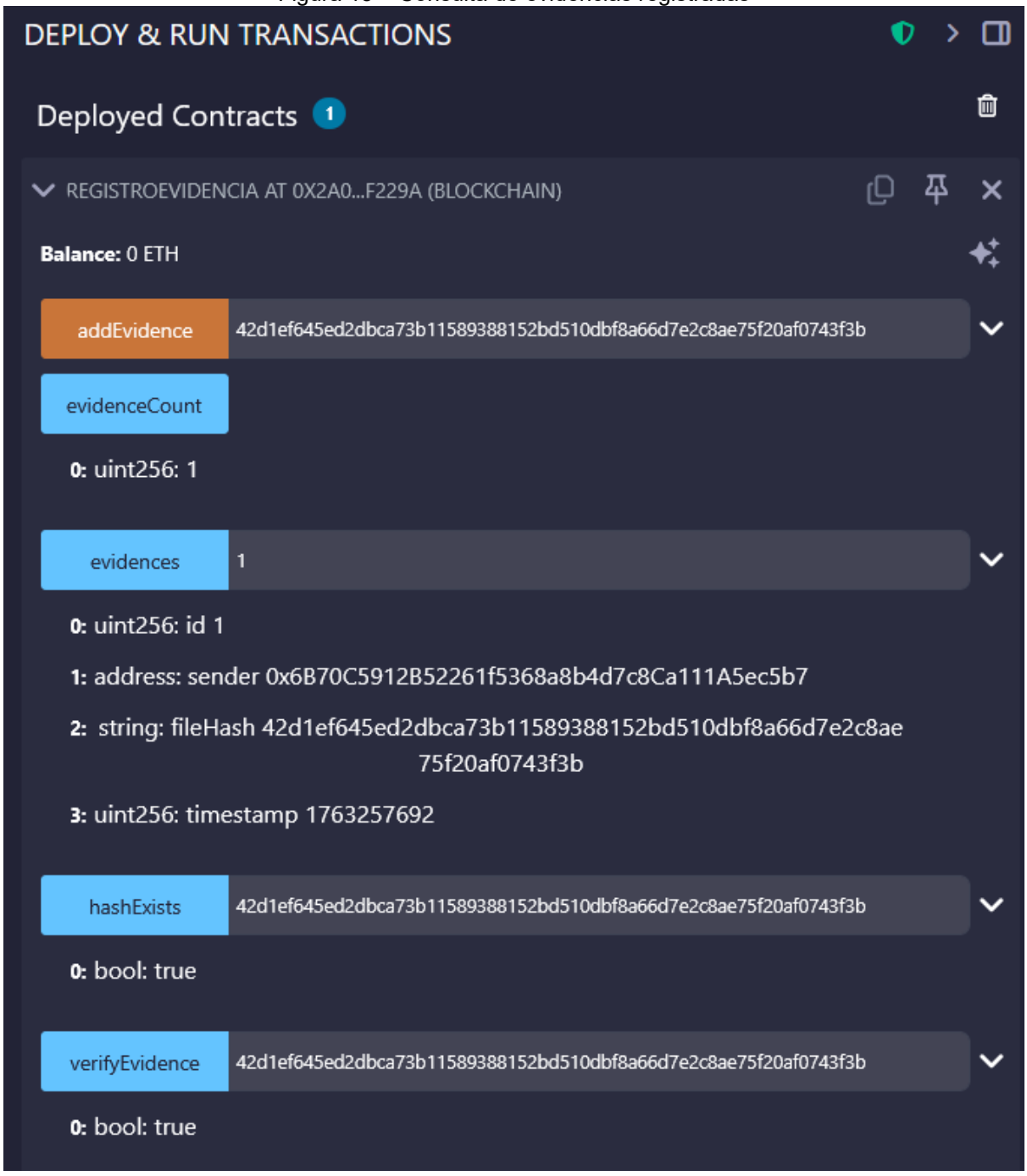


Fonte: Autoria própria (2025)

É possível consultar o registro diretamente pelo Remix ao informar o identificador associado à evidência armazenada. A figura 14 representa a consulta, que retorna informações como o hash original, endereço de origem e o timestamp em UNIX. Ademais, o contrato oferece a possibilidade de verificar a existência de um hash por meio da função *verifyEvidence()*, onde o valor informado é comparado aos

registros armazenados e, caso esteja presente, a função resulta em “*true*”, permitindo confirmar rapidamente se a evidência está registrada.

Figura 15 – Consulta de evidências registradas



Fonte: Autoria própria (2025)

4. CONSIDERAÇÕES FINAIS

A implementação prática de um contrato inteligente demonstrou a viabilidade técnica da utilização da tecnologia de *blockchain* para a manutenção da integridade de evidências digitais. Através da rede de teste Ethereum Sepolia, do ambiente de desenvolvimento Remix IDE e da carteira MetaMask, foi possível construir um fluxo funcional de inclusão e consulta de hashes de arquivos digitais para garantir transparência, autenticidade e imutabilidade de registros. O processo de criação, compilação e implantação do contrato ocorreu corretamente, com suas funções principais permitindo registrar o hash das evidências na *blockchain* por meio da função *addEvidence()*, com identificadores como o endereço de origem e *timestamp*, e recuperar informações armazenadas com a função *getEvidence()*, confirmando a integridade e consistência dos dados.

De forma geral, a demonstração prática confirma que contratos inteligentes podem ser utilizados como base para sistemas de cadeia de custódia digital, garantindo que qualquer alteração no arquivo original possa ser detectada ao comparar o hash calculado com o que foi registrado na rede *blockchain*. O projeto apresentou uma prova de conceito funcional, com o intuito de demonstrar, em ambiente controlado, como a tecnologia *blockchain* pode servir como mecanismo de preservação da integridade de evidências digitais, criando um repositório imutável de evidências sem armazenar o arquivo em si, e de simples implementação quando comparado a modelos como o desenvolvido por Alruwaili (2021) intitulado "*CustodyBlock: A Distributed Chain of Custody Evidence Framework*". Em seu trabalho, o modelo proposto é baseado em uma infraestrutura de *blockchain* privada, o Hyperledger Fabric, tendo sido concebido para uso em ambientes forenses e governamentais, com participantes autorizados e contratos inteligentes para automatizar o controle de evidências.

A comparação entre o protótipo desenvolvido e o modelo CustodyBlock evidencia diferenças significativas quanto à complexidade, infraestrutura necessária e abrangência funcional. Enquanto o protótipo apresentado neste trabalho possui caráter didático e foco no registro imutável de evidências digitais por meio de seus hashes, o Custody Block foi projetado como um sistema completo de cadeia de custódia, incorporando autenticação de usuários, controle de acesso, metadados detalhados e logs contínuos de manipulação da evidência.

Portanto, os resultados mostram que a *blockchain* é uma tecnologia capaz de preservar a integridade de evidências digitais, fornecendo registros imutáveis, verificáveis e resistentes a adulterações. Enquanto o modelo original do CustodyBlock (Alruwaili, 2021) fornece uma base conceitual robusta para aplicações reais, o protótipo desenvolvido neste trabalho cumpre o papel de materializar e testar esses conceitos de forma acessível, validando sua viabilidade técnica.

REFERÊNCIAS

ALRUWAILI, Fahad F. CustodyBlock: a distributed chain of custody evidence framework. Information, [S.L.], v. 12, n. 2, p. 88, 20 fev. 2021. MDPI AG. http://dx.doi.org/10.3390/info12020088.

ANDONI, Merlinda; ROBU, Valentin; FLYNN, David; ABRAM, Simone; GEACH, Dale; JENKINS, David; MCCALLUM, Peter; PEACOCK, Andrew. *Blockchain technology in the energy sector: a systematic review of challenges and opportunities.* ***Renewable And Sustainable Energy Reviews***, [S.L.], v. 100, p. 143-174, fev. 2019. Elsevier BV. http://dx.doi.org/10.1016/j.rser.2018.10.014.

BACK, A. Hashcash: *A denial of service counter-measure*. 2002. Disponível em: http://www.hashcash.org/hashcash.pdf. Acesso em: 12 jun. 2025.

CHAQUIAN FILHO, Elias; DUARTE, Sara Luize Oliveira; LACERDA, Liluyoud Cury de. A IMPORTÂNCIA DA PRESERVAÇÃO DA EVIDÊNCIA DIGITAL NOS CRIMES CIBERNÉTICOS. Diálogos: Economia e Sociedade, Porto Velho, v. 2, n. 2, p. 89-109, 7 dez. 2018. Disponível em: https://periodicos.saolucas.edu.br/index.php/dialogos/article/view/50/39. Acesso em: 15 maio 2025.

CHICARINO, Vanessa R. L.; JESUS, Emanuel Ferreira; ALBUQUERQUE, Célio V. N. de; ROCHA, Antônio A. de A. Uso de *blockchain* para privacidade e segurança em IoT. In: **Anais do XXXV Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC 2017)**. Belém: Sociedade Brasileira de Computação, 2017. p. 63–76. Disponível em: https://www.sbrc2017.ufpa.br/sessao/uso-de-blockchain-para-privacidade-e-seguranca-em-iot/. Acesso em: 15 nov. 2025.

ETHEREUM FOUNDATION. ***What is Ethereum?*** 2025. Disponível em: https://ethereum.org/pt-br/what-is-ethereum/. Acesso em: 15 nov. 2025.

ETHERSCAN. Blockchain Explorer for Ethereum. Disponível em: https://etherscan.io. Acesso em: 15 nov. 2025.

GOOGLE CLOUD. Web3 Faucet. Disponível em: https://cloud.google.com/application/web3/faucet. Acesso em: 15 nov. 2025.

GUIMARÃES, Ricardo Ferreira de Alencastro. *Guia para criação de smart contracts no Ethereum*. Trabalho de Conclusão de Curso (Bacharelado em Ciência da Computação) – Universidade de Caxias do Sul, Caxias do Sul, 2024.

HASSAN, Nihad A. Perícia Forense Digital. São Paulo: Novatec, 2019. Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=Uq-rDwAAQBAJ&oi=fnd&pg=PA20&dq=per%C3%ADcia+forense+digital&ots=ZyCHSrlagI&sig=ii7bP5alDKG0sy38ZlJsj6GByaw&redir_esc=y#v=onepage&q=per%C3%ADcia%20forense%20digital&f=true. Acesso em: 6 maio 2025.

HINTZBERGEN, Jule et al. Fundamentos de Segurança da Informação: com base na iso 27001 e na iso 27002. 3. ed. São Paulo: Brasport, 2018. 190 p.

LUNARDI, Roben Castagna; MICHELIN, Regio Antonio; ZORZO, Avelino Francisco; ANDRADE, Ewerton; KREUTZ, Diego. Introdução a *Blockchain*: Visão Geral e Conceitos Básicos. **Unihacker: Tecnologias e Desafios em Cibersegurança I**, [*s. l*], p. 73-100, dez. 2024.

MIRANDA, Júlio César de; ZUCHI, Jederson Donizete. TECNOLOGIA *BLOCKCHAIN*. **Revista Interface Tecnológica**, [S.L.], v. 15, n. 2, p. 457-469, 30 dez. 2018. Interface Tecnologica. http://dx.doi.org/10.31510/infa.v15i2.376. Disponível em: https://revista.fatectq.edu.br/interfacetecnologica/article/view/376. Acesso em: 26 maio. 2025.

MERRIAM-WEBSTER. *Nonce*. Disponível em: https://www.merriam-webster.com/dictionary/nonce. Acesso em: 30 maio 2025.

METAMASK. Your home in web3. 2025. Disponível em: https://metamask.io/. Acesso em: 16 nov. 2025.

NAKAMOTO, S. Bitcoin: *A peer-to-peer electronic cash system*., 2008. Disponivel em: http://www.bitcoin.org/bitcoin.pdf. Acesso em: 30 maio 2025.

NIST. *Hash Functions* | CSRC. Disponível em: <https://csrc.nist.gov/projects/hash-functions>. Acesso em: 26 maio. 2025.

PORTO, Lucas Magno de Oliveira; GLÓRIA, Luciano Ribeiro Tambasco; FERREIRA, Mariah Brochado. Contratos inteligentes na *Blockchain*: validade e restrições. *Universidade Federal de Minas Gerais*, 14 fev. 2022. Artigo de periódico. Disponível em: https://repositorio.ufmg.br/items/541367de-da3a-4b89-b851-d0fd6cf92080. Acesso em: 16 nov. 2025.

REMIX PROJECT. Remix – Ethereum IDE. Disponível em: https://remix.ethereum.org. Acesso em: 15 nov. 2025.

SANTOS, Adriano José Sousa; BORGES, Andre Felipe Miranda; RODRIGUES, Gustavo Luís Mendes Tupinambá. A CADEIA DE CUSTÓDIA NA COLETA DA PROVA DIGITAL DE ACORDO COM A LEI 13.964/2019, DOS SEUS ARTIGOS 158-A AO 158-F. Recima21 - Revista Científica Multidisciplinar - Issn 2675-6218, São Paulo, v. 2, n. 8, p. 77-91, 6 set. 2021. Disponível em: https://recima21.com.br/index.php/recima21/article/view/612/521. Acesso em: 06 jun. 2025.

SANTOS, Lucas Melo dos; PICOLO, Eduardo Nunes. **Aplicação descentralizada de votação aberta usando *blockchain* Ethereum**. 2023. 76 f. TCC (Graduação) - Curso de Engenharia de Software, Universidade de Brasília, Faculdade Unb Gama, Brasília, 2023. Disponível em: https://bdm.unb.br/bitstream/10483/39171/1/2023_LucasSantos_EduardoPicolo_tcc.pdf. Acesso em: 15 nov. 2025.

SOUZA, Gustavo Toledo de. Aplicação da tecnologia *blockchain* na autenticidade de documentos. 2023. Trabalho de Conclusão de Curso (Bacharelado em Engenharia de Computação) – Escola Politécnica, Pontifícia Universidade Católica de Goiás, Goiânia, 2024.

TAHERDOOST, Hamed. *Smart Contracts in Blockchain Technology: A Critical Review*. Information, v. 14, n. 2, p. 117, 2023. DOI: 10.3390/info14020117. Disponível em: https://www.mdpi.com/2078-2489/14/2/117. Acesso em: 12 nov. 2025.

YAGA, Dylan; MELL, Peter; ROBY, Nik; SCARFONE, Karen. *Blockchain Technology Overview*. Gaithersburg, MD: National Institute of Standards and Technology, 2018. (NISTIR 8202). Disponível em: https://doi.org/10.6028/NIST.IR.8202. Acesso em: 28/10/2025.

ZHANG, Rui; XUE, Rui; LIU, Ling. *Security and privacy on blockchain*. *ACM Computing Surveys*, v. 52, n. 3, p. 1–34, 2019. DOI: 10.1145/3316481. Acesso em: 15 nov. 2025.

ZOTTELE, William Lorenzoni; LONDERO, Fabrício Tonetto; VIEIRA, Sylvio André Garcia; CANAL, Ana Paula. *Reformulação de um sistema de financiamento coletivo em um contrato inteligente na blockchain da rede Ethereum*. *Disciplinarum Scientia: Série Naturais e Tecnológicas*, v. 24, n. 3, p. 171–190, 2023. DOI: 10.37779/nt.v24i2.4701.