UNIVERSIDADE FEDERAL DO AMAZONAS

FACULDADE DE TECNOLOGIA

PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA

Vivianne de Aquino Rodrigues

CONTRATO INTELIGENTE MULTIASSINATURA SERIAL APLICADO A FINS EMPRESARIAIS

Manaus

2024

CONTRATO INTELIGENTE MULTIASSINATURA SERIAL APLICADO A FINS EMPRESARIAIS

Vivianne de Aquino Rodrigues

Dissertação apresentada ao Programa de Pós-Graduação em Engenharia Elétrica da Universidade Federal do Amazonas, como parte dos requisitos para obtenção do título de Mestre em Engenharia Elétrica.

Orientador: Prof. Dr. Carlos Augusto de Moraes Cruz.

Este trabalho corresponde à versão final da Dissertação defendida por Vivianne de Aquino Rodrigues e orientada pelo Prof. Dr. Carlos Augusto de Moraes Cruz.

.

Manaus

2024

Ficha Catalográfica

Ficha catalográfica elaborada automaticamente de acordo com os dados fornecidos pelo(a) autor(a).

Rodrigues, Vivianne de Aquino
R696c Contrato Inteligente Multiassinatura Serial aplicado a fins empresariais. / Vivianne de Aquino Rodrigues . 2024
82 f.: il. color; 31 cm.

Orientador: Carlos Augusto de Moraes Cruz
Dissertação (Mestrado em Engenharia Elétrica) - Universidade Federal do Amazonas.

1. Blockchain. 2. Contrato Inteligente. 3. Multiassinatura. 4. Aplicações. 5. Segurança. I. Cruz, Carlos Augusto de Moraes. II. Universidade Federal do Amazonas III. Título

Ministério da Educação
Universidade Federal do Amazonas
Coordenação do Programa de Pós-Graduação em Engenharia Elétrica

FOLHA DE APROVAÇÃO

Poder Executivo Ministério da Educação
Universidade Federal do Amazonas
Faculdade de Tecnologia
Programa de Pós-graduação em Engenharia Elétrica

Pós-Graduação em Engenharia Elétrica. Av. General Rodrigo Octávio Jordão Ramos, nº 3.000 - Campus Universitário, Setor Norte - Coroado, Pavilhão do CETELI. Fone/Fax (92) 99271-8954 Ramal:2607. E-mail: ppgee@ufam.edu.br

VIVIANNE DE AQUINO RODRIGUES

CONTRATO INTELIGENTE MULTIASSINATURA SERIAL APLICADO A FINS EMPRESARIAIS

Dissertação apresentada ao Programa de Pós-Graduação em Engenharia Elétrica da Universidade Federal do Amazonas, como requisito parcial para obtenção do título de Mestre em Engenharia Elétrica na área de concentração Controle e Automação de Sistemas.

Aprovada em 27 de agosto de 2024.

BANCA EXAMINADORA

Prof. Dr. Carlos Augusto de Moraes Cruz-Presidente
Prof. Dr. José Frederico da Silva Pinagé - Membro Titular 1 - Externo
Prof. Dr. Waldir Sabino da Silva Junior - Membro Titular 2 - Interno

Manaus, 23 de agosto de 2024.

Documento assinado eletronicamente por **Carlos Augusto de Moraes Cruz**, **Coordenador**, em 09/09/2024, às 11:14, conforme horário oficial de Manaus, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Frederico da Silva Pinagé**, **Professor do Magistério Superior**, em 09/09/2024, às 14:07, conforme horário oficial de Manaus, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015

Documento assinado eletronicamente por **Waldir Sabino da Silva Júnior**, **Professor do Magistério Superior**, em 10/09/2024, às 12:18, conforme horário oficial de Manaus, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://sei.ufam.edu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **2204369** e o código CRC **4517B739**.

Av. Octávio Hamilton Botelho Mourão - Bairro Coroado 1 Campus Universitário Senador Arthur Virgílio Filho, Setor Norte - Telefone: (92) 3305-1181

CEP 69080-900 Manaus/AM - mestrado_engeletrica@ufam.edu.br

Referência: Processo nº 23105.036187/2024-92

SEI nº 2204369

Criado por 31183646291, versão 2 por 31183646291 em 23/08/2024 09:56:08.

AGRADECIMENTOS

À Deus, digno de toda honra e louvor, por Ele tudo foi feito e é graças a Ele que cheguei até aqui. Agradeço também a Maria Santíssima, minha Mãe das Graças, por toda a sua intercessão, sei que as bênçãos que recebo passam pelas tuas mãos.

A meus pais Lucilene Silva de Aquino e Gilberto Vieira de Aquino (em memória), por sempre acreditarem no meu potencial e por todo apoio, incentivo, proteção e dedicação a mim concedidos durante a vida toda. Jamais conseguiria sem vocês!

Agradeço particularmente ao meu esposo Jadson Rodrigues, que caminha ao meu lado, me ama, me ampara e me faz ir além. Obrigada pelo apoio diário, pelo colo e por toda motivação! Você é minha melhor decisão de vida e meu maior incentivador! Amo você!

Agradeço ao Grupo de Oração Jovem Nossa Senhora de Pentecostes por todo apoio espiritual e por me fazerem enxergar as maravilhas de Deus mesmo nos momentos mais difíceis.

Agradeço de maneira especial ao meu orientador professor Dr. Carlos Augusto, por toda sua dedicação na orientação desse estudo, sua amizade e por todo o conhecimento, não só técnico, mas também moral que me transmitiu. Obrigada por acreditar no meu potencial e por abraçar comigo, esse trabalho com tanto empenho!

Agradeço ao Sidia Instituto de Ciência e Tecnologia, em especial ao meu time ATLAS, por todo suporte durante as minhas ausências e por priorizarem meus estudos.

Agradeço aos professores examinadores deste trabalho, pela disponibilidade e pelas contribuições. Por fim, agradeço a Universidade Federal do Amazonas e a todos os professores do curso, dos quais tive a honra de ser aluna.

FRASE MOTIVACIONAL

Jesus parou e mandou que lho trouxessem. Chegando ele perto, perguntou-lhe: Que queres que te faça? Respondeu ele: “Senhor, que eu veja”. (Lc 18, 40-41)

Resumo da dissertação apresentada ao Programa de Pós-Graduação em Engenharia Elétrica da Universidade Federal do Amazonas, como parte dos requisitos necessários para a obtenção do grau de Mestre em Engenheira Eletricista.

CONTRATO INTELIGENTE MULTIASSINATURA SERIAL APLICADO A FINS EMPRESARIAIS

Vivianne de Aquino Rodrigues

Agosto/2024

Orientador: Prof. Dr. Carlos Augusto de Moraes Cruz
Curso: Mestrado em Engenharia Elétrica.

A tecnologia blockchain pode revolucionar a maneira como as empresas controlam seus negócios, podendo prover soluções para meios de pagamentos seguros, identificação digital e contratos empresariais. Através desse trabalho foi possível integrar diversas áreas de conhecimento, buscando unir conceitos de redes blockchain e contratos inteligentes. Este estudo propõe uma solução, que utiliza a tecnologia Blockchain, para a criação de um sistema de contrato inteligente com multiassinatura de forma serial, sendo inovador pois os participantes não precisam estar logados simultaneamente na mesma plataforma para assinar o contrato. Possui o intuito de mostrar o uso e eficácia das redes blockchain em aplicações empresariais, além de realizar um estudo sobre segurança dessas redes através de uma prova de conceito com Smart Contracts, que supera as limitações e inseguranças das plataformas tradicionais de assinaturas de contratos. Para a criação da interface do contrato utilizou-se a plataforma de desenvolvimento de contratos inteligentes Full Stack Web3 sCrypt-TS, que possibilita ao usuário criar o contrato de maneira ágil e segura. Para assegurar os aspectos relacionados à segurança, foram realizados testes, em diferentes cenários e por fim é gerado uma análise dos resultados encontrados. Com isso, constatou-se que a solução desenvolvida atende as exigências de segurança e confidencialidade do mercado empresarial, bem como possibilita inúmeras pesquisas e aplicações.

Palavras-chave: Blockchain; Contrato Inteligente; Multiassinatura; Aplicações; Segurança.

Summary of the dissertation presented to the Postgraduate Program in Electrical Engineering at Federal University of Amazonas, as part of the requirements necessary to obtain the Master's degree in Electrical Engineering.

SERIAL MULTI SIGNATURE SMART CONTRACT APPLIED TO BUSINESS PURPOSES

Vivianne de Aquino Rodrigues

August/2024

Advisor: Prof. Dr. Carlos Augusto de Moraes Cruz

Course: Master's degree in Electrical Engineering.

Blockchain technology can revolutionize the way companies manage their businesses, providing solutions for secure payment methods, digital identification, and corporate contracts. Through this work, it was possible to integrate several areas of knowledge, seeking to unite concepts of blockchain networks and smart contracts. This study proposes a solution, which uses Blockchain technology, to create a smart contract system with serial multi-signature, being innovative because the participants do not need to be logged in simultaneously on the same platform to sign the contract. The aim was to demonstrate the possibility of using and the effectiveness of blockchain networks in business applications, in addition to conducting a study on the security of these networks. To create the contract interface, the Full Stack Web3 sCrypt-TS smart contract development platform was used, which allows the user to create the contract in an agile and secure way. To ensure security-related aspects, tests were carried out in different scenarios and finally an analysis of the results found was generated. After all the tests were carried out, it was found that the developed solution meets the security and confidentiality requirements of the business market, as well as enabling numerous research and applications.

Keywords: Blockchain; Smart Contract; Multisignature; Applications; Security.

SUMÁRIO

LISTA DE ABREVIATURAS E SIGLAS

NFT - Token Não-Fungível, do inglês *Non-Fungible Token.*

BTC - Bitcoin

DLT - Tecnologia de registro distribuídos, do inglês *Distributed Ledger Technology.*

CPF – Cadastro de Pessoa Física.

eDSL – Linguagem Específica de Domínio Incorporada, do inglês *embedded Domain Specific Language.*

SHA - Secure Hash Algorithm

SAT - Satoshis

TXID - Transaction Identication

UTXO – Saída de transação não gasta, do inglês *Unspent Transaction Output.*

IoT – Internet das Coisas, do inglês *Internet of Things.*

BSV – Bitcoin SV, do inglês *Bitcoin Satoshi Vision.*

LGPD – Lei Geral de Proteção de Dados (Lei 13.709).

P2PKH - Pagar para Hash de Chave pública, do inglês *Pay To Public Key Hash.*

POW - Proof of Work

P2P - Peer-to-peer

LISTA DE FIGURAS

LISTA DE TABELAS

CAPÍTULO 1 – INTRODUÇÃO

1.1 JUSTIFICATIVA

Segurança de dados é primordial em todos os aspectos da sociedade atual. Dentro do universo das inovações tecnológicas, a busca por soluções para os problemas do cotidiano e a necessidade de segurança no mundo digital, foi um dos motivos que desencadeou a expansão do conceito de Blockchain e por conseguinte, dos contratos inteligentes, do inglês Smart Contracts.

A blockchain é uma tecnologia que está sendo cada vez mais usada globalmente, não apenas para criptomoedas, mas também em muitos outros setores, como: sistemas de pagamento, medicina e saúde, armazenamento em nuvem, educação, seguros, imóveis, entretenimento, agricultura, indústria 4.0 etc [1,2].

De modo que, a tendência é o crescimento da utilização dessas redes, expandindo-se a diferentes aplicações em diversas áreas. Para isso acontecer é necessário ter uma compreensão profunda dos seus conceitos e potenciais, tornando-se de fundamental importância estudar e compreender como estabelecer transações em uma blockchain, suas vantagens e como funciona os algoritmos de segurança [3]. Afinal, antes de uma tecnologia tornar-se amplamente utilizada, é necessário entender a complexidade técnica de sua adoção, a regulamentação em torno da tecnologia e quão robusta a infraestrutura deverá ser, para fins de escalabilidade.

Afinal, conceitos como escalabilidade em aplicações envolvendo Blockchain, são cruciais para o bom desempenho e a utilização dessa rede. Atualmente, a escalabilidade é uma das principais preocupações no campo da tecnologia blockchain e uma área de pesquisa ativa. Pois habilita a Blockchain a receber, validar e armazenar um volume muito grande de transações com grandes quantidades de dados, o que a torna flexível para o desenvolvimento de uma infinidade de aplicações [4].

Por sua vez, os contratos inteligentes são geralmente referidos como contratos digitais que permitem que duas partes assumam alguma forma de troca, tais como: transferência de dinheiro, propriedades, NFTs e etc. Isso causa impacto em vários setores industriais em todo mundo, pois abre caminho para um sistema descentralizado, possibilitando que a blockchain e os contratos inteligentes assumam todos os aspectos do futuro [5,6].

Nota-se um interesse, por parte de várias empresas, de adotarem o uso de contratos inteligentes em seus modelos de negócio. Existem diversas notícias mostrando que alguns

bancos digitais no Brasil, estão em fase de testes na Blockchain para negociações e transações de seus clientes. Outros exemplos reais consistem em testes na Blockchain para ativos e bens, como carros usados, pagamentos e investimentos envolvendo criptomoedas [7,8].

Baseado nisso, este trabalho visa incluir um olhar aprofundado sobre as possibilidades que as redes blockchain fornecem e como os contratos inteligentes são formados. Seu diferencial consiste justamente nesse foco aplicado aos conceitos envolvendo contratos inteligentes, o estudo de características técnicas, algoritmos de segurança e os principais elementos que compõem e permitem esse elo entre blockchain e contratos inteligentes.

Dado que em 2022, foram vazados 257 terabytes de dados no mundo, onde 43% desses vazamentos ocorreram somente no Brasil. O mais alarmante é que cerca de 35% do total de dados expostos, foi devido à desproteção de bancos de dados. [9]. Dito isso, o principal motivador para esse projeto provém de problemas ocasionados pela utilização ineficaz da LGPD (Lei Geral de Proteção de dados) nos contratos empresariais [10], que acarreta vazamentos de informações sigilosas ou sensíveis. Através dos contratos inteligentes é possível assegurar a proteção dos dados pessoais, sendo uma solução muito atraente para as demandas e/ou contratos empresariais.

Diante desse contexto, esse trabalho descreve uma proposta de criação de um contrato inteligente multiassinatura serial, utilizando a Blockchain SV, para aplicações empresariais, com uma prova de conceito utilizando *Smart Contracts* que supera as limitações e inseguranças das plataformas tradicionais de assinaturas de contratos. Além de expor suas características e vantagens, para mostrar as soluções e possibilidades que esse projeto oferece ao mercado, não excluindo as exigências impostas pela rede blockchain e como ela está estruturada.

1.2 OBJETIVOS

1.2.1 Objetivo Geral

Propor uma solução, que utiliza a tecnologia Blockchain, para um sistema de contrato inteligente com multiassinatura, de forma serial. De maneira que os participantes não precisam estar logados simultaneamente na mesma plataforma para assinar o contrato, sua principal característica inovadora. Possui também o intuito de mostrar a possibilidade de uso e eficácia das redes blockchain em diversas aplicações e realizar um estudo sobre segurança dessas redes.

1.2.2 Objetivos Específicos

I. Apresentar fundamentação teórica sobre redes blockchain, características, componentes, algoritmos de consenso e particularidades de segurança.
II. Definir os contratos inteligentes existentes e suas particularidades, fazer um estudo comparativo entre eles, enfatizando os contratos multiassinaturas e considerando métricas de performance.
III. Construir contrato inteligente de multiassinatura serial, norteando a interligação desses conceitos. E apresentar as principais vantagens e desvantagens entre o modelo proposto (serial) e o modelo existente (paralelo), de acordo com o cenário escolhido (empresarial).
IV. Montar uma interface de contrato inteligente utilizando uma plataforma web, justificando a utilização da solução desenvolvida em detrimento aos modelos de assinaturas digitais existentes.
V. Realizar testes usando a solução desenvolvida, na rede blockchain através de uma plataforma pública para monitorar os testes realizados, apresentando os resultados atingidos.

1.3 PROCEDIMENTOS METODOLÓGICOS

Para alcançar os objetivos esperados, o presente trabalho foi desenvolvido a partir das seguintes etapas:

ETAPA 1 - Elaboração do referencial teórico necessário: Nesta etapa foi realizado o levantamento de referências para a elaboração da fundamentação teórica sobre os conceitos acima mencionados. As informações foram obtidas a partir da utilização de livros, sites, dissertações, teses, monografias e artigos relacionados ao assunto.

ETAPA 2 - Ambientação com a linguagem *sCrypt*, responsável pela construção do contrato inteligente: Nessa etapa foi executado um estudo aprofundado sobre essa linguagem para embasamento do código construído no projeto.

ETAPA 3 - Construção do código do contrato multiassinatura serial e desenvolvimento da interface web utilizada para compor a proposta desse estudo.

ETAPA 4 - Testes e resultados obtidos com os códigos construídos: análise do comportamento nos cenários avaliados, com o intuito de compreender os desafios envolvendo uma aplicação específica (contratos empresariais), suas exigências e características.

1.4 ESTRUTURA DO TRABALHO

O presente trabalho contém cinco capítulos, sendo organizado da seguinte forma: O Capítulo 1 descreve a justificativa do trabalho e seus objetivos geral e específicos, bem como a metodologia utilizada na elaboração da pesquisa. O Capítulo 2 aborda todos os conceitos primordiais da rede blockchain, algoritmos de consenso e técnicas utilizadas. O Capítulo 3 aborda informações essenciais sobre smart contracts. O Capítulo 4 apresenta um estudo sobre segurança de dados pessoais, incluindo o porquê da escolha dessa aplicação. O Capítulo 5 descreve os cenários de teste com a ferramenta pronta e também descreve as características dos contratos desenvolvidos nesse estudo, focando na análise dos resultados obtidos durante os testes.

CAPÍTULO 2 – AS REDES BLOCKCHAIN

A tecnologia blockchain não é em sua essência uma novidade, visto que desde 1991 há relatos de estudos de Stuart Haber e W. Scott Stornetta sobre a criação de uma rede de blocos criptografados, onde não era possível adulterar registros de data e hora dos documentos [1]. Aqui entra então o conceito de *timestamp* , ou seja, o momento em que a ocorrência do evento é registrada por um computador, em vez do momento do evento em si. Normalmente, ele registra a data e a hora do dia em que o evento ocorreu e é preciso para uma pequena fração de segundo [1, 11]. No ano seguinte (1992), atualizaram seu sistema incorporando árvores Merkle, visando aumentar eficiência e permitindo a coleta de mais documentos em um único bloco [1].

Todavia, o primeiro conceito de blockchain público, utilizado como base especificamente para bitcoin, nasceu em 2008, no artigo acadêmico: *Bitcoin, um sistema financeiro eletrônico peer-to-peer,* publicado por uma pessoa (ou grupo) sob o pseudônimo de Satoshi Nakamoto [2,12]. Este artigo explora possibilidades de uso da tecnologia blockchain com criptomoedas, inclusive citando os artigos de Haber e Stornetta. Nakamoto forneceu detalhes de como a tecnologia estava bem equipada para melhorar a confiança digital, focada na descentralização e imutabilidade, o que deixa claro não ser possível controlar completamente a rede.

Em linhas gerais pode-se definir a Blockchain como um banco de dados, tratando-se de uma tecnologia que agrupa conjuntos de informações que se conectam por meio de um sistema de *hashes* que viabiliza o encadeamento seguro e coeso de blocos de informações. Também pode ser entendida como uma DLT (*Distributed ledger technology*), cujo funcionamento consiste em um livro de registros, aberto e descentralizado, que permite a realização confiável e segura de qualquer transação entre duas ou mais pessoas, sem a necessidade de intermediários, através da Internet [13].

Como forma de ilustrar o que é uma blockchain, da mesma forma, pode-se imaginar um livro-razão (digital), similar a um sistema contábil, onde todos os registros de transações estão escritos e os participantes de uma mesma rede de computadores seriam todos portadores de uma cópia. Para manter a imutabilidade de longo prazo do blockchain em ambientes com permissão, a blockchain fornece prova irreversível e incontestável de confirmações de bloco. É crucial manter a blockchain imutável para garantir a confiabilidade dos aplicativos de negócios

que dependem dela [14]. Vale ressaltar que essa rede não tem um controle central e pode ser acessada de vários pontos por qualquer pessoa dependendo do seu tipo de implementação.

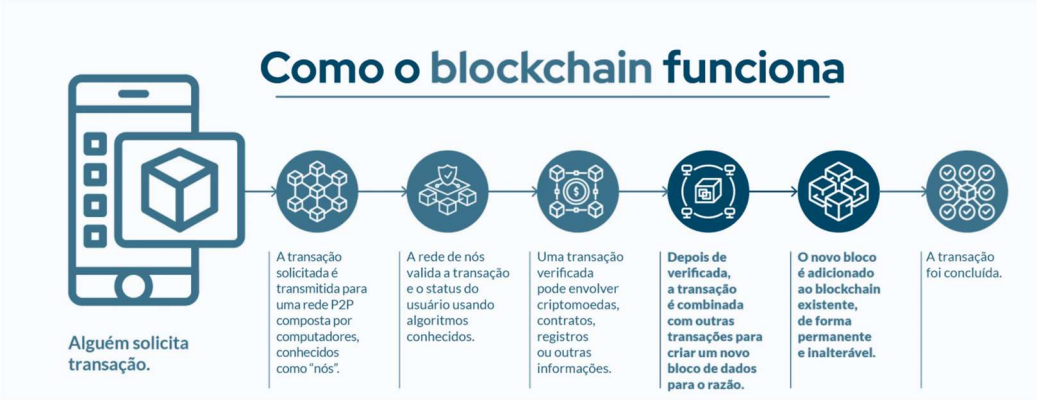


Figura 1 - Funcionamento da Blockchain.
Fonte: Adaptado de [15].

Sendo um serviço de registro distribuído no formato peer-to-peer (par-a-par), a blockchain pode ser traduzida em uma corrente de blocos, onde se registram transações de forma segura. De modo que, o bloco posterior vai conter a impressão digital do anterior mais seu próprio conteúdo e, com essas duas informações, gerar sua própria impressão digital, ou seja, o conteúdo do registro só pode ser atualizado adicionando outro bloco vinculado ao bloco anterior.

É importante definir de que forma esses blocos estão organizados dentro da Blockchain. Pode-se dizer que os blocos, de acordo com [13], contêm as informações de:

- Data e hora de processamento: o que controla quando o bloco foi processado (minerado), e permite uma ordem cronológica na leitura da sequência de dados;
- Quantidade transacionada: correspondente aos valores contidos em cada transação, por exemplo: em bitcoin para a rede BTC, ou em Ether (ETH), para a rede Ethereum;
- Partes da transação: ao invés de usar dados pessoais como nome ou CPF, são utilizados scripts que identificam a origem e o destino dos fundos nas transações, os tipos mais populares de scripts são aqueles de endereços digitais;
- *Hashes* únicas: identificam cada transação de forma individual, também são conhecidas como *transaction ID* ou TXID.

Todos esses blocos possuem um *hash* (id), ou seja, uma identificação. Sendo assim, os blocos dentro da blockchain são compostos por todas as transações ocorridas na rede, sendo uma transação, o menor componente de um bloco.

A Blockchain, em outras palavras, é uma plataforma onde as pessoas podem realizar transações de todos os tipos sem a necessidade de um árbitro central ou confiável, tal como um banco ou uma instituição governamental. A inovação da Blockchain se deu justamente nesse ponto: o armazenamento de dados de forma sequencial, sem a necessidade de uma entidade coordenando o processo [13].

Isso é essencial quando se busca alternativas para o setor bancário, por exemplo. De acordo com [13], afirma-se que a aplicação de blockchain ao setor bancário poderia mudar fundamentalmente a forma como os ativos são armazenados e mantidos, as obrigações são cumpridas, os contratos são executados e os riscos geridos. A tecnologia blockchain promete construir sistemas seguros de transferência de valor, agilizar processos de negócios, aumentar a transparência e facilitar a auditabilidade, reduzindo assim a lacuna de confiança. O estudo elaborado em [16], mostra o potencial de reduzir custos de transações, custo de reconciliação, custo de compensação, custo de processamento e custo geral de liquidação. Além disso, a blockchain poderia promover a redução de riscos inerentes às atividades de PCS (Sistemas de Compensação e Liquidação de Pagamentos), como riscos legais e de liquidação, riscos operacionais, tais como fraude e riscos financeiros, liquidez ou riscos de contraparte.

Na Figura 2 pode-se ver a diferença entre blockchain, DLTs e bancos de dados tradicionais.

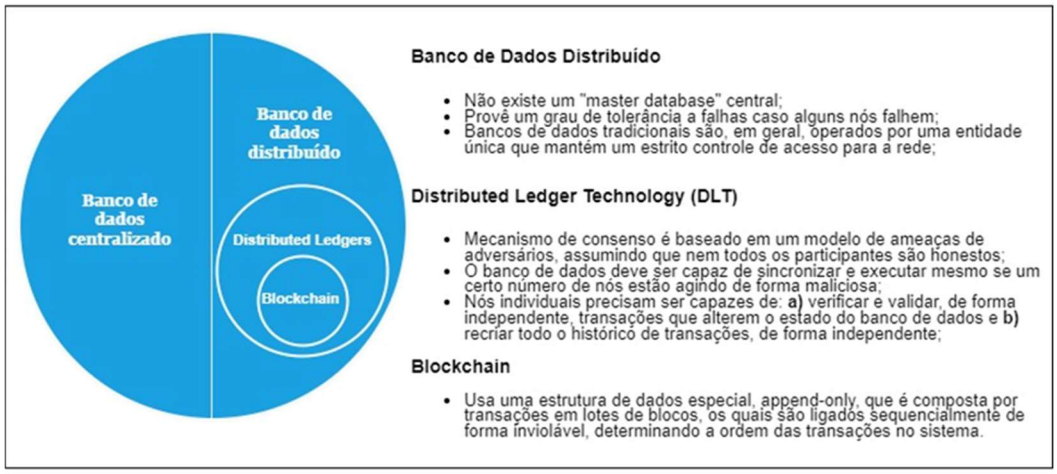


Figura 2 - Comparação entre Blockchain e outros tipos de bancos de dados.
Fonte: Adaptado de [1].

Adiante veremos mais detalhadamente as características da blockchain, suas implementações e peculiaridades.

2.1 Características das Redes Blockchain

As características primordiais das redes Blockchain entregam confiança e consenso dentro de um cenário de total transparência, com a perenidade dos dados garantida por uma infraestrutura descentralizada e distribuída [1]. Como diferenciais das redes blockchain pode-se pontuar:

- Segurança – É uma rede extremamente difícil de violar, desde que o protocolo seja seguido pela maioria dos participantes; Provê a segurança de uma informação que é pública;
- Confiabilidade para o sistema (rede auditável) – Trata-se de uma infraestrutura pronta para uso;
- Custo – O custo se justifica, pois, não há necessidade de construir a segurança e infraestrutura para redundância do banco de dados;
- Estabilidade e Escalabilidade.

2.1.1 Segurança e Proteção das Transações Instantâneas

O que tange o aspecto de segurança em redes blockchain é o baixo potencial de inviolabilidade, fato que se baseia em fatores tecnológicos e legais. O primeiro é fruto do poder de *hash* que controla a blockchain, o segundo se baseia no protocolo utilizado e na responsabilidade de alguma entidade para representar o sistema e extinguir sinistros. De acordo com [1] a Blockchain garante a autenticidade e integridade das transações, partindo da impossibilidade de qualquer tipo de alteração, evitando duplicidade de informações. O banco de dados criado é compartilhado entre os participantes da rede de maneira transparente, onde todos podem acessar seu conteúdo. O gerenciamento do banco de dados é feito de forma autônoma usando redes *peer-to-peer* e um servidor de registro de data e hora.

Um bloco contém informações sobre uma transação, cabeçalho e várias informações. Estas são armazenadas na seção de detalhes da transação [17]. Um bloco também contém um número de *hash*, que é gerado com base nas informações da transação. Caso haja alguma alteração nessas informações da transação, o número do *hash* será significativamente diferente. Portanto, se um bloco for violado, as modificações podem ser facilmente identificadas. Um bloco contém não apenas seu próprio número de *hash*, mas também o número de *hash* do bloco

anterior. Por causa disso, os blocos se conectam e formam uma cadeia. Todas essas características são sustentadas pela estrutura técnica da blockchain [17].

A proteção de transações instantâneas permite que os usuários tenham a segurança de que, uma vez suas transações tenham sido enviadas para a *mempool* da rede, estas possam ser prontamente utilizadas para a criação de novas transações antes mesmo de serem confirmadas em um bloco do sistema. Todas as ferramentas criptográficas utilizadas pelo protocolo Bitcoin proporcionam um grau de segurança ímpar ao sistema, que tem passado por todos os testes ao longo dos anos desde a sua concepção.

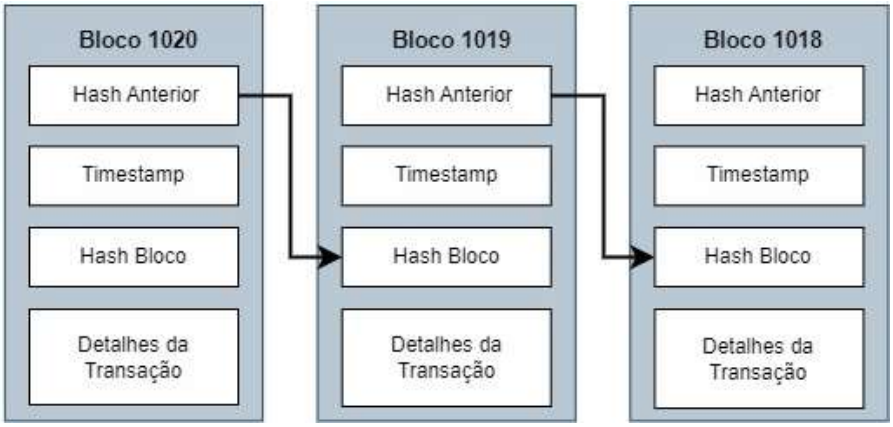


Figura 3 - Funcionamento dos blocos na Blockchain.
Fonte: Adaptado de [1].

2.1.2 Confiabilidade

A blockchain pode ser usada para qualquer transação, pública ou privada, com igual eficiência, desde que sejam observados os critérios específicos de cada ambiente [1].

Por conta dessa característica, a blockchain possibilita os chamados *smart contracts*, que consistem em um protocolo distribuído que executa os termos de um contrato de forma autônoma com o objetivo de reduzir o risco de erro e manipulação. A possibilidade de criação desses contratos, permite em sua essência, aumentar a confiabilidade do sistema. A execução de um contrato inteligente, na forma de um código executável, permite que os membros da rede executem tal código de acordo com os termos descritos no contrato.

Os contratos inteligentes, estabelecem um relacionamento digital entre duas partes, sendo um tipo de transação que também é registrado na Blockchain. Com a introdução desse conceito de contratos inteligentes, tornou-se possível a automatização de processos. Isso é tão

significativo que permite saltar do universo das transações simples e aplicações limitadas, para uma gama de possibilidades.

2.1.3 Custo

Quando é feita uma análise de custo de uma blockchain, basicamente considera-se duas vertentes: custo de transação e custos de execução [18]. Os custos de transação são baseados no envio de dados para a blockchain, por exemplo, no caso de um contrato inteligente, os custos de transação dependerão do tamanho do contrato e quantidade de informações. Os custos de execução se baseiam nas operações computacionais executadas como resultado das transações. Estes custos também são relacionados com armazenamento de variáveis globais e tempo de execução dos códigos – processamento. A rigor, o custo total seria a soma desses dois valores [18].

Ao se pensar nesse contexto, o custo de usar blockchain pode parecer elevado, porém quando se analisa mais profundamente, descobre-se que todo o custo é justificável pelos seguintes motivos: com a blockchain não é necessário construir mecanismos de segurança e infraestrutura de rede, bem como investimentos relacionados a construção de redundância do banco de dados. Problemas estes, comuns ao utilizar plataformas prontas para gerenciamento e controle de redes IoT, por exemplo.

2.1.4 Estabilidade e Escalabilidade

A estabilidade de uma blockchain depende do uso de um protocolo coeso, fortemente testado, que não seja alterado desde a sua concepção, permitindo aos desenvolvedores a segurança de que suas aplicações estão sendo desenvolvidas em uma plataforma que não sofrerá alterações ao longo dos anos.

A escalabilidade habilita a Blockchain a receber, validar e armazenar um volume muito grande de transações com grandes quantidades de dados, o que a torna flexível para o desenvolvimento de uma infinidade de aplicações. O dos principais desafios é atingir escalabilidade, segurança e descentralização ao mesmo tempo [19].

Abaixo foram reunidas algumas características básicas da blockchain segundo os autores:

Característica	Descrição	Autor
Transparência	É possível ter a visualização de qualquer transação.	Kshetri (2017a); (Park, 2018)
Descentralização	Não há a necessidade de um órgão intermediário que aprove a transação ou que determine certos regulamentos de contrato.	Lee, et al (2017)
Segurança	O banco de dados é imutável, em outras palavras, consiste em um registro que não pode ser alterado, revisado ou adulterado, nem mesmo para aqueles que operam o banco de dados.	Jillepalli, et al (2017)
Consenso	A validação de uma transação requer que outros computadores de outros participantes entrem em um consenso para possibilitar que essa transação ocorra.	Pîrlea (2018)
Automatização	O software foi desenvolvido para que não haja duplicidade ou informação conflituosa, sendo assim, transações que não respeitem essa regra não são registradas dentro da blockchain.	Goldenfein (2018)
Confiabilidade	A capacidade de manter os registros íntegros e confiáveis é sustentada pela estrutura técnica da blockchain.	(Ying; Jia; DU, 2018)

Tabela 1: Características básicas da blockchain identificadas na literatura.
Fonte: Adaptado de [1].

2.2 Blockchain, base para criptomoedas

Antes de compreender a ligação entre os conceitos blockchain e criptomoedas, faz-se necessário compreender e conceituar o bitcoin. De maneira geral, pode-se defini-lo como uma criptomoeda, ou seja, uma moeda não apenas criptografada, como também virtual. Esse sistema é descentralizado, não existindo, portanto, um vínculo com governo ou entidade pública, bancos ou empresas privadas. O Bitcoin usa a Blockchain como uma forma de resolver os problemas

existentes há muito tempo de gasto duplo de dinheiro digital e processamento de transações digitais de forma descentralizada, sem a necessidade de terceiros confiáveis [11].

O tamanho da blockchain do bitcoin está perto de atingir 5.450 gigabytes em 2024, já que o banco de dados tem um crescimento exponencial de quase um gigabyte em poucos dias. O blockchain do Bitcoin contém uma lista continuamente crescente e inviolável de todas as transações e registros do Bitcoin desde seu lançamento inicial em janeiro de 2009.

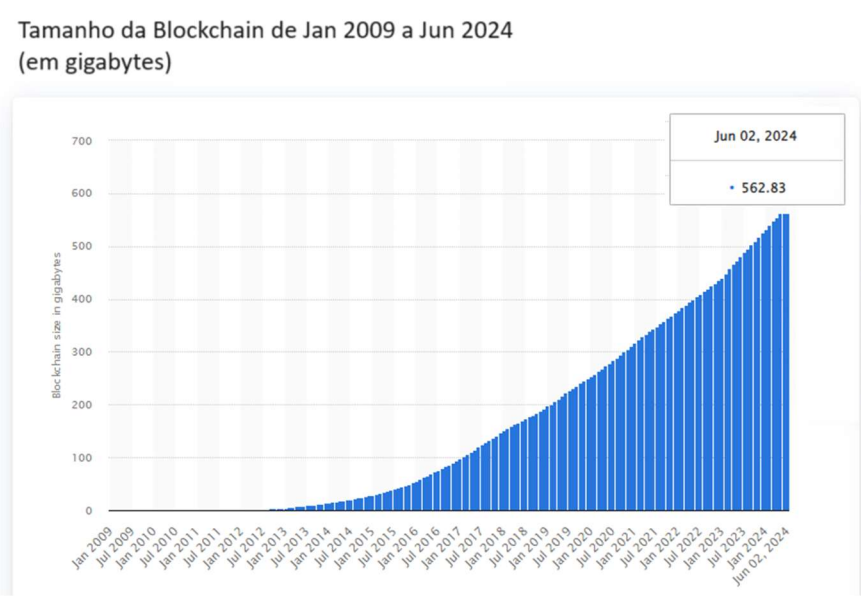


Figura 4 - Tamanho da Blockchain (BTC)
Fonte: Adaptado de [20].

Idealizado para ser um sistema econômico alternativo, todas as informações são controladas e verificadas pelos próprios usuários através da tecnologia blockchain. No caso, um Bitcoin é um arquivo digital que funciona como uma moeda alternativa que possui o mesmo valor a nível mundial. Nesse contexto, a blockchain fornece meios para armazenar todas as informações sobre as transações de Bitcoins, funcionando como um banco de dados seguro e acessível a todos os usuários.

Para aprofundar nesse conteúdo, as próximas sessões descrevem os algoritmos de consenso usados para verificação da Blockchain, que buscam validar de maneira segura, as movimentações que ocorrem na rede.

2.3 Algoritmos de Consenso

Os algoritmos de Prova (Proof ofs) são algoritmos utilizados na verificação e validação das transações que ocorrem no universo da Blockchain. Cada tipo de algoritmo preza por 3

princípios básicos, são eles: uso de energia, segurança e escalabilidade [21]. Podemos destacar os principais algoritmos na lista abaixo:

a. Proof of Work;
b. Proof of Stake;
c. Proof of Reserve;
d. Proof of History.

Com o intuito de manter a veracidade e a segurança da rede, eles possuem algumas particularidades que serão mencionadas a seguir. Vale ressaltar que o foco deste trabalho está no Proof of Work, pois ele é a base para o funcionamento do bitcoin. Todavia, na Seção 2.3.3 será apresentado um resumo dos quatro algoritmos de consenso através de uma tabela comparativa.

2.3.1 Proof of Work (PoW)

De acordo com [17,22], o PoW foi criado como objetivo principal a criação de um método eficaz de combate aos e-mails de spam, envolvendo funções vinculadas à memória, reduzindo o risco de poluição de mensagens. O Proof of Work se destaca por sua segurança, sendo quase impossível que haja ataques ou transações fraudulentas circulando na rede.

A verificação das transações de criptomoedas usando o algoritmo Proof of Work é feita por meio da mineração. Os mineradores competem para consolidar o bloco em que estão trabalhando, e validar transações para ganhar recompensas em cada bloco validado. Dessa forma, o Proof of Work garante que os blocos não possam ser adicionados à blockchain sem executar o trabalho necessário.

A construção dos blocos acontece mediante algumas regras, tais como: as transações são agrupadas respeitando o tamanho máximo que um bloco pode comportar, e apenas transações que sejam verificadas como válidas devem fazer parte do bloco.

Enquanto as transações esperam em fila para serem adicionadas em algum bloco, elas ficam temporariamente em uma estrutura chamada de pool [23]. Os computadores da rede competem entre si para ver quem consegue encontrar um bloco válido primeiro dentro da pool. O computador que encontra um bloco válido avisa os demais para que se faça a checagem e que haja um consenso de validação. Para que uma transação seja considerada verídica, ela precisa ser verificada e validada. Para estabelecer a função de *hash*, o Bitcoin usa o algoritmo

de *hash* SHA-256, responsável por converter qualquer sequência de caracteres em uma sequência de 64 caracteres ou números.

2.3.2 Vantagens e Desvantagens do PoW

Conforme já dito anteriormente, uma das principais vantagens do *Proof of Work* é a segurança, pois esse algoritmo garante que os blocos não sejam adicionados à rede Blockchain sem a execução de um trabalho necessário. Uma vez que isso acontece, não apenas a transação é marcada como válida, mas também é postada no blockchain público para que todos tenham acesso. Portanto não é viável por exemplo, que um nó malicioso valide facilmente todos os blocos para adicionar informações inconsistentes. Caso haja tentativa de fraude, outros participantes da rede saberiam e descartariam esse bloco inválido. A criação de Satoshi Nakamoto foi construir um sistema que permite que todos os participantes se concentrem na mesma verdade de forma independente. Portanto, temos que o *PoW* é fundamental para que isso aconteça.

A notável inovação da blockchain do Bitcoin previne o problema de gasto duplo em redes P2P sem depender de uma parte centralizada. Isso se torna possível devido à saída de transação não gasta (*UTXO*), que é um modelo que define a saída não gasta, que é a entrada para a próxima transação na rede blockchain [17, 24].

A principal desvantagem do uso do *PoW* está em exigir uma quantidade significativa de energia para realizar a mineração [23]. Nesse contexto, a necessidade de supercomputadores pode acarretar uma centralização do sistema de mineração, devido a tendência de que a mineração seja concentrada aos grandes grupos. Entretanto, vale ressaltar, que isso não afeta a descentralização das transações que continuam sendo realizadas em um sistema *P2PKH*, além disso gera-se uma demanda por equipamentos mais eficientes energeticamente, que realimentam a cadeia produtiva, gerando pesquisa e desenvolvimento contínuo.

Em adição a isso temos o quesito tempo de verificação, pois verificar blocos usando PoW leva alguns minutos, impactando por exemplo transações múltiplas e rápidas. Isso passa a ser um problema para redes que não se preocupam em garantir a proteção de transação instantâneas, ou seja, aquelas que podem ter seus *UTXOs* utilizados mesmo antes da confirmação destas em um bloco.

2.3.3 Algoritmos de Consenso: Tabela Comparativa

Algoritmo de consenso	Vantagens	Desvantagens
Proof of Work (PoW)	Alto grau de segurança, devido a mineração. Utiliza poder computacional para verificar se as transações são válidas;	Requer uma grande quantidade de energia para efetuar a mineração, dentro de um contexto de equipamentos ineficientes energeticamente.
Proof of Stake (PoS)	Não requer um poder de processamento tal qual o PoW necessita para ser executado.	Receio de centralizar as riquezas nas mãos dos mais ricos; Requer investimento inicial mais pesado; Brechas na segurança - devido a não exigir um gasto energético.
Proof of Reserve (PoR)	Promete que empresas podem assegurar suas solvências; Maior a transparência entre os clientes e os serviços;	Tende a possuir brechas na prova de passivos - As 'exchanges' podem omitir alguns passivos para 'enganar' um atestado de PoR;
Proof of History (PoH)	Promete habilitar duas grandes linhas de frente: baixas taxas e escalabilidade.	Risco iminente de centralização, pois atualmente a rede possui apenas 1200 validadores; Limitação em seu desempenho - durante estresse na rede; Ataques na segurança;

Tabela 2: Comparação entre Algoritmos de Consenso.
Fonte: A Autora.

2.4 Componentes da Blockchain

Entender como a blockchain está dividida, auxilia o processo de utilização da tecnologia. A Figura 5 mostra os componentes da tecnologia blockchain:

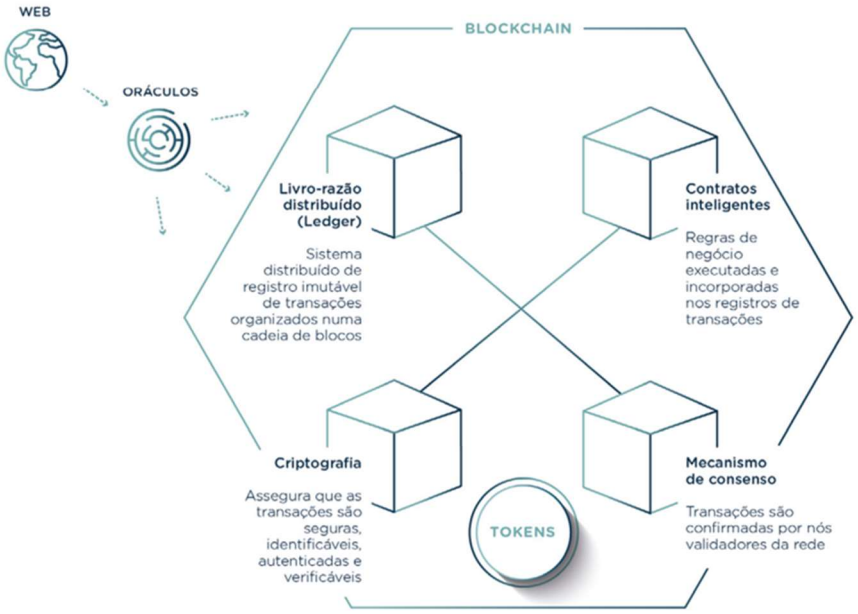


Figura 5 - Componentes de uma rede Blockchain.
Fonte: [25]

O foco principal do próximo capítulo são os contratos inteligentes, como estão estruturados, suas vantagens e aplicações. Esta ideia foi proposta em 1997, por Nick Saab, possuindo quase a mesma idade da Internet [26], porém apenas com o desenvolvimento da blockchain, tornou-se possível o suporte para a operação de contratos inteligentes propriamente dito [27].

CAPÍTULO 3 – CONTRATOS INTELIGENTES (SMART CONTRACTS)

O intuito desse capítulo é apresentar conceitos importantes envolvendo o universo dos contratos inteligentes, do inglês *smart contracts*. De acordo com [25], os contratos inteligentes, são código-fonte em linguagem de programação (*scripts*), que podem ser definidos e autoexecutados em uma infraestrutura de blockchain ou DLT, sem a necessidade de intermediários, tais como: bancos ou cartórios.

Outro conceito proveniente da União Internacional de Telecomunicações (ITU), define contrato inteligente como um programa de computador que utiliza transações assinadas criptograficamente em uma rede DLT [25]. O contrato inteligente é executado pelos nós e os resultados da execução são validados por consenso e registrados no livro-razão distribuído. A automação inteligente de contratos reduz custos e riscos de erros, mitiga riscos de fraude e, potencialmente, otimiza muitos processos de negócios [25].

O algoritmo do contrato inteligente é equivalente ao jurídico, com relação a prestação das obrigações com seus termos, condições ou encargos. Sendo elaborados pelos próprios contratantes ou prestadores de serviços por eles contratados. Na elaboração do algoritmo encontra-se a inteligência do contrato, ou seja, o contrato inteligente na blockchain introduz o algoritmo jurídico no processamento eletrônico do contrato, possibilitando declarações, negócios, transações e pagamentos descentralizados, invioláveis, autênticos, seguros e transparentes, seja entre os contratantes em si, seja entre os contratantes e uma empresa contratada para a execução do contrato inteligente [28].

De acordo com [25], um contrato inteligente pode ser caracterizado pelo atingimento de 4 objetivos principais:

a) Observabilidade: característica responsável por verificar os envolvidos no contrato cumpriram sua parte;
b) Verificabilidade: possibilidade de haver reclamação de uma das partes envolvidas, em caso de não-cumprimento ou violação do contrato;
c) Privacidade: o conhecimento sobre o conteúdo e a execução do contrato deve ser distribuído apenas entre as partes envolvidas;
d) Obrigatoriedade: Execução de forma obrigatória, conforme programado em seu código-fonte, sem margem para duplicidade de informações.

A Tabela 3 mostra as principais vantagens relacionadas a utilização de contratos inteligentes:

Característica	Vantagens
Transparência	Podem ser escritos e verificados a qualquer momento por todas as partes envolvidas.
Eficiência	Menor prazo para execução, devido a eliminação dos passos manuais torna a execução do contrato mais rápida.
Precisão	Execução é descrita por um algoritmo computacional, isso a torna precisa, desde que não aja erros de programação.
Segurança	A infraestrutura DLT garante a segurança em contratos inteligentes. Aliado a isso tem-se as assinaturas digitais, provenientes de chaves criptográficas. Isso torna o contrato inviolável.
Rastreabilidade	Os dados de cada execução das funções do contrato ficam armazenados, permitindo que a execução do contrato seja auditável a qualquer momento.
Economia	Em razão da eliminação de intermediários, tais contratos reduzem custos de execução.
Confiança	As partes envolvidas no contrato podem usar essa tecnologia de maneira segura e transparente, aumentando o nível de confiança.

Tabela 3: Vantagens da utilização de contratos inteligentes.
Fonte: A autora.

Há uma infinidade de aplicações possíveis para *smart contracts*, abrangendo diversas áreas, pois com eles podem ser feitos investimentos, empréstimos, seguros, compra e venda de itens, transferências etc. Também existe a possibilidade aplicações descentralizadas incluindo: jogos, eleições, saúde, energia, gestão imobiliária, e muitas outras áreas. Isso é devido aos benefícios envolvendo segurança e transparência, facilitando a relação, o gerenciamento e a negociação entre fornecedor e consumidor [29].

3.1 Ciclo de Vida de um Smart Contract

De acordo com [30], os contratos inteligentes possuem um ciclo de vida muito similar ao dos contratos tradicionais, o que inclui 3 partes: Geração do contrato, liberação do contrato e execução do contrato, conforme ilustrado na Figura 6:

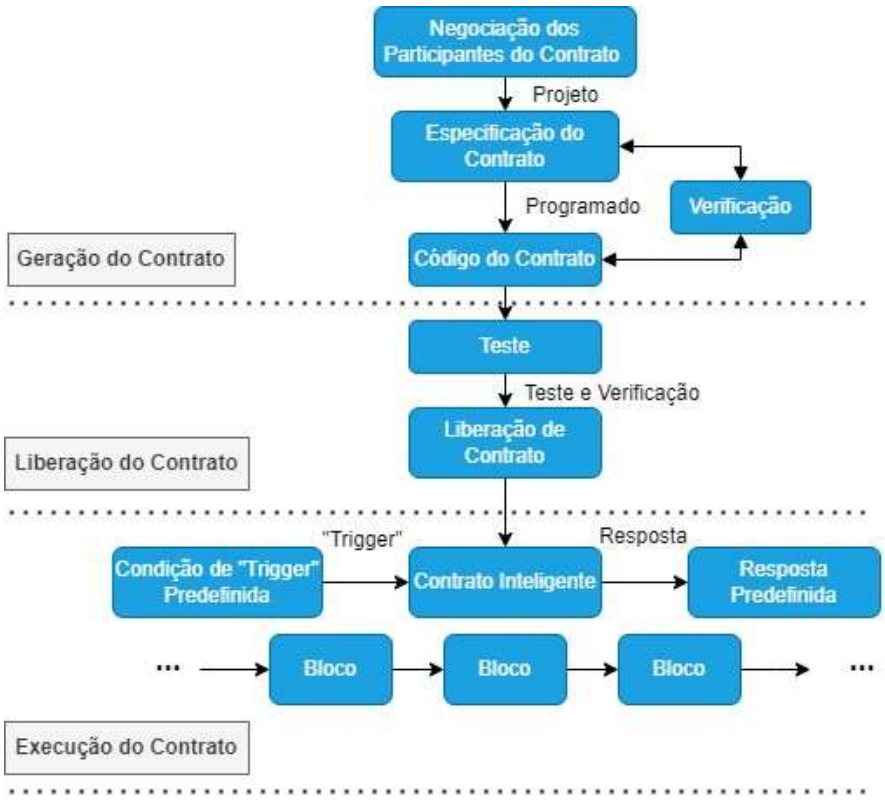


Figura 6 - Ciclo de Vida de um Smart Contract.
Fonte: Traduzido de [30].

a) Geração do contrato: Essa etapa é formada por 4 itens, conforme ilustrado na Figura 6. Formada pela negociação do contrato, formulação da especificação do contrato, verificação do contrato e aquisição do código do contrato [30]. Ou seja, os participantes do contrato negociam, esclarecem os direitos e obrigações de ambas as partes, determinam o texto padrão do contrato e programam esse texto, obtendo assim o código padrão do contrato após verificação.
b) Liberação do Contrato: Esse processo é semelhante à liberação do contrato. O contrato assinado é distribuído a cada nó por meio de P2P, que irão armazenar temporariamente o contrato recebido na memória, e aguardarão o consenso. De acordo com [30], o processo de consenso é implementado da seguinte forma: cada nó irá empacotar os

contratos armazenados temporariamente no período recente em um conjunto de contratos, calcular o valor *hash* do conjunto e, finalmente, montar o valor *hash* do conjunto de contratos em um bloco e espalhar para outros nós de toda a rede; O nó que recebe o bloco compara o valor *hash* armazenado nele com o valor *hash* armazenado no conjunto de contratos. Após várias rodadas de envio e comparação, todos os nós finalmente chegarão a um consenso sobre o contrato recém-lançado, e o conjunto de contratos acordado será distribuído a todos os nós de toda a rede na forma de bloco [30].

c) Execução do contrato: Essa etapa é baseada em um mecanismo de "acionamento por evento" ou evento *trigger*. Todos os contratos inteligentes baseados em blockchain contêm mecanismos de processamento e salvamento de transações, tal como uma máquina de estado para aceitar e processar vários contratos inteligentes. De acordo com [30], o contrato inteligente percorrerá a máquina de estado e acionará as condições de cada contrato, após isso enviará o contrato que atende às condições de acionamento para a fila a ser verificada. O contrato a ser verificado é distribuído para cada nó e, como acontece com uma transação blockchain normal, o nó é primeiro assinado e verificado para garantir a validade do contrato, e o contrato verificado é executado com sucesso após um consenso ser alcançado. Todo o processo de processamento do contrato é concluído automaticamente pelo sistema de contrato inteligente integrado ao blockchain subjacente, que é aberto e transparente e não pode ser adulterado [30].

3.2 Multiassinaturas em Smart Contracts

A assinatura eletrônica formaliza o processo entre a oferta e a aceitação dos contratantes, e atualmente é considerada a ferramenta para a celebração de um contrato, garantindo seu valor jurídico [31]. É uma solução que permite assinar qualquer documento, por exemplo: orçamentos, acordos, contratos, e outros, eletronicamente. As vantagens são muitas, podendo-se destacar, a agilidade nos processos relacionados à assinatura de um documento e arquivação digital desses documentos assinados. A combinação entre a assinatura eletrônica e os contratos inteligentes torna possível a redução drástica de conflitos de interesses e fraudes.

Um contrato multiassinado, é uma forma de compartilhar a propriedade de UTXO entre vários participantes [32]. Esse método de armazenamento é frequentemente utilizado por empresas, organizações e parceiros (sócios), para estabelecer a propriedade sobre um conjunto

de fundos. A razão pela qual esse tipo de contrato é chamado multiassinatura ou *multisig,* se deve ao fato da necessidade de múltiplas assinaturas de endereços diferentes para que uma transação seja executada. Esses endereços pertencem a pessoas diferentes, e podem ser armazenados em carteiras de hardware, baseadas em chaves privadas.

Os contratos 'Multisig' possuem várias vantagens, podendo-se destacar:

- Evitar um único ponto de falha, tornando significativamente mais difícil o comprometimento dos fundos;
- Dividir a responsabilidade de propriedade de um endereço e seus fundos entre várias pessoas;

Em adição a essas vantagens também vale ressaltar a possibilidade de definir uma porcentagem para garantir o consenso de uma transação. Por exemplo, se 50% dos envolvidos concordarem e assinarem o contrato, o contrato é válido. Em um cenário em que existem múltiplas chaves anexadas a um contrato 'multisig' e apenas uma parte maioritária dos proprietários das chaves precisa aprovar uma transação, não importa se um indivíduo perde a sua chave, pois haverá outros indivíduos que poderão aprovar a transação [32]. Isso viabiliza as empresas de estabelecer regras de participação em ações, decisões e outras aplicações.

3.2.1 Tipos de contratos inteligentes multiassinatura

Esquemas de múltiplas assinaturas (multisig) podem ser implementados de duas maneiras principais: serial (sequencial) e paralela (concorrente). Na prática, a escolha entre assinaturas seriais e paralelas depende frequentemente dos requisitos e restrições específicas da aplicação ou sistema e pode influenciar o design e a complexidade da implementação. Alguns sistemas podem usar uma combinação de ambas as abordagens para diferentes estágios de um processo. A escolha ideal pode depender do caso de uso específico e dos requisitos dos participantes envolvidos.

Em uma abordagem simples, cada um dos *n* usuários possuirá um par de chaves pública/privada. Uma assinatura válida nesse caso, é uma coleção de assinaturas de *n* usuários. A verificação das assinaturas requer o uso da chave pública de cada signatário para verificar a assinatura final. A escolha entre os dois tipos de contrato pode ser baseada também em implicações de segurança, podendo depender dos requisitos de segurança específicos do caso

de uso. A nível de comparação, é possível considerar a dificuldade de comprometer uma assinatura versus comprometer múltiplas assinaturas simultaneamente.

A diferença entre os tipos de contrato se dá principalmente na forma como o contrato é executado. Com a multiassinatura em paralelo, por exemplo, o contrato só inicia sua execução, quando as assinaturas estão presentes, ou seja, não há a possibilidade de executar o contrato sem que a quantidade mínima de assinaturas seja atingida. Este tipo de contrato pode também ser considerado como contrato de um único estado, mas também pode ser chamado de contrato sem estado (*stateless*), já que finaliza na primeira execução.

Enquanto na multiassinatura serial, o contrato pode ser executado assim que é feita a primeira assinatura, deixando registrado na rede o momento exato que houve a assinatura, a ordem delas e seus parâmetros individuais. Cada assinatura gera um TX ID do contrato, possibilitando que o processo todo seja dinâmico. Este tipo de contrato pode ser classificado como contrato de estados, pois a cada evento pelo qual o contrato passa, é gerado um novo estado que possui todas as características do contrato gênesis e o estado atual. A finalização de um contrato de estados é apenas uma opção dentro do universo de possibilidade de estados futuros.

Na Tabela 4 é possível observar as principais vantagens dos dois tipos de contratos com multiassinatura.

Serial	Paralela
Ordem controlada: As assinaturas seriais implicam uma ordem específica na qual as assinaturas devem ser aplicadas. Isto pode ser vantajoso em situações em que a ordem de aprovação é importante.	**Processamento Simultâneo:** Em um esquema paralelo, todas as assinaturas necessárias podem ser obtidas simultaneamente. Isso pode levar a tempos de processamento de transações mais rápidos em comparação com uma abordagem serial.
Rastreabilidade: A natureza sequencial das assinaturas facilita o rastreamento do processo de aprovação. Fica claro quem assinou primeiro, segundo e assim por diante, o que pode ser benéfico para fins de auditoria, mesmo quando uma ordem fixa de assinaturas não seja um requisito.	**Atraso reduzido:** Os signatários em um esquema paralelo não precisam esperar pela conclusão das assinaturas anteriores. Isso pode reduzir atrasos em processos urgentes.

Dependência de assinaturas anteriores: Num esquema em série, os signatários posteriores podem tomar a sua decisão com base nos resultados das assinaturas anteriores. Isso permite aprovações ou rejeições condicionais.	**Assinaturas Redundantes e Descentralização:** Em alguns casos, assinaturas paralelas podem fornecer redundância. Assinaturas paralelas podem apoiar um processo de tomada de decisão mais descentralizado, pois cada parte pode aprovar ou rejeitar a transação de forma independente.
Fluxo de trabalho estruturado: A abordagem serial fornece um fluxo de trabalho estruturado, que pode ser benéfico em cenários onde é necessário um processo de aprovação claro e linear.	**Tomada de decisões independente:** Os signatários podem tomar as suas decisões independentemente uns dos outros, proporcionando flexibilidade na tomada de decisões.

Tabela 4: Vantagens de contratos inteligentes com multiassinatura serial x paralela.
Fonte: A autora.

3.3 Linguagens de Programação utilizadas em Smart Contracts

Conforme dito anteriormente, para a geração de um smart contract faz-se necessário escrever um código funcional que possua toda a especificação do contrato. Para isso, existem atualmente diversas ferramentas e linguagens de programação que podem auxiliar nesse processo.

Assim como existem diversas tecnologias Blockchain, existem diferentes linguagens de programação de contratos inteligentes desenvolvidas especificamente para esse fim. As linguagens mais populares usadas na programação de contratos inteligentes são: Solidity, TypeScript (sCrypt), Vyper, JavaScript, C++, Yul, Rust, Phyton, Scilla entre outras [33].

É importante ressaltar a importância do Solidity no processo de popularização de contratos inteligentes, pois a maioria dos elementos de um contrato Solidity são semelhantes aos da linguagem Java; entretanto, Solidity é uma linguagem de programação orientada a objetos projetada essencialmente para o desenvolvimento de contratos inteligentes [33].

As implementações que o Solidity suporta são específicas de contratos (o que inclui atributos, funções completas, eventos e todo o código que executa a lógica para atingir o objetivo do contrato). As bibliotecas são um tipo de contrato, implantados em endereços específicos, e outros contratos podem. reutilizar suas propriedades e métodos [33].

Com isso, o Solidity permitiu criar contratos inteligentes complexos e diversos, como tokens, exchanges descentralizadas, plataformas de empréstimo e jogos. O Solidity também se

beneficiou do crescimento do ecossistema Ethereum, que forneceu ferramentas, bibliotecas, estruturas e padrões para facilitar o desenvolvimento, teste, implantação e interação de contratos inteligentes.

A popularização do uso do Solidity, também desencadeou alguns desafios e limitações, seja com relação a linguagem em si, quanto a própria plataforma Ethereum. Por exemplo, um dos principais desafios se deu na garantia de segurança e correção dos contratos inteligentes. Outro desafio foi lidar com os problemas de escalabilidade e eficiência do Ethereum, que limitaram o rendimento e a velocidade dos contratos inteligentes e aumentaram a taxa necessária para executar transações na rede. Um terceiro desafio foi acompanhar a inovação e a concorrência no espaço blockchain, à medida que novas plataformas e linguagens surgiam, oferecendo diferentes recursos e compensações para o desenvolvimento de contratos inteligentes.

Neste trabalho, por estarmos utilizando a rede Bitcoin, optou-se pela linguagem sCrypt, que é uma eDSL baseada em TypeScript para escrever contratos inteligentes em Bitcoin SV. Sendo uma linguagem de alto nível para ser compilada em Bitcoin Script, que exporta um submódulo chamado 'BSV' que é uma interface capaz de gerenciar coisas de baixo nível para a blockchain do Bitcoin, como criar pares de chaves, construir, assinar e serializar transações Bitcoin.

A linguagem sCrypt é estritamente um subconjunto do TypeScript, portanto, todo o código sCrypt é em sua essência um código TypeScript válido [34]. No próximo capítulo será descrito o modelo de contrato inteligente 'Multisig' desenvolvido, e como o código do contrato foi estruturado fazendo uso da plataforma sCrypt.

3.4 A rede Bitcoin SV

A proposta de contrato inteligente desenvolvida neste trabalho, utiliza a blockchain da rede Bitcoin Satoshi Vision (BSV), pois é o protocolo original proposto por Satoshi Nakamoto. Essa rede disponibiliza todos os elementos necessários para o desenvolvimento de *smart contracts* em uma blockchain pública, sendo comprometida com a estabilidade, escalabilidade, segurança e transações instantâneas protegidas.

A estabilidade é fornecida ao sistema pelo uso de um protocolo coeso, fortemente testado ao longo dos anos, que não foi alterado desde a sua concepção, permitindo aos

desenvolvedores, a segurança de que suas aplicações estão sendo desenvolvidas em uma plataforma que não sofrerá alterações ao longo dos anos. A quantidade de transações na rede BSV, por dia pode ser verificada através do gráfico abaixo:

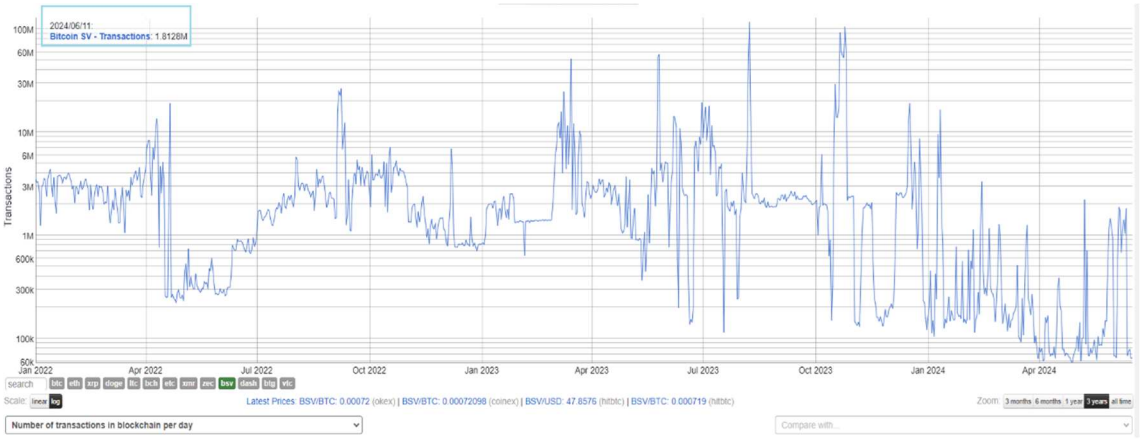


Figura 7 - Quantidade de transações por dia, na rede BSV.
Fonte: Adaptado de [35].

O compromisso com a escalabilidade habilita a rede a receber, validar e armazenar transações com grandes quantidades de dados, o que a torna flexível para o desenvolvimento de uma infinidade de aplicações. Todas as ferramentas criptográficas utilizadas pelo protocolo Bitcoin proporcionam um grau de segurança ímpar ao sistema, que tem passado por todos os testes ao longo dos anos desde a sua concepção. O compromisso com a proteção de transações instantâneas permite que os usuários tenham a segurança de que, uma vez suas transações tenham sido enviadas para a Mempool da rede, estas possam ser prontamente utilizadas para a criação de novas transações antes mesmo de serem confirmadas em um bloco do sistema. A blockchain da rede BSV é pública, o que fornece toda a transparência necessária para qualquer tipo de auditoria a que o sistema seja submetido. Dentre a miríade de aplicações que podemos desenvolver na rede, temos smart contracts, NFTs, registros temporais de qualquer tipo de documento, entre outros.

Outra grande vantagem da rede é o baixíssimo custo de rede para a execução de qualquer tipo de transação, o que abre as portas para uma infinidade de aplicações de baixo custo. Isso se deve a escalabilidade da rede, sendo capaz de realizar 50.000 transações por segundo. Naturalmente, ao multiplicar as transações por segundo, você reduz o custo de energia por transação [36].

O desenvolvimento dos Smart Contracts utilizará a linguagem de programação sCrypt, que possui todos os recursos necessários para o desenvolvimento de smart contracts na blockchain BSV e possui sintaxe muito semelhante à linguagem Javascript.

De acordo com [58], podemos resumir as vantagens da rede BSV da seguinte forma:

Benefícios da rede BSV	
Transações ponto a ponto	O BSV permite transações diretas entre as partes sem a necessidade de um terceiro confiável, reduzindo os custos de transação e aumentando a eficiência.
Taxas de transação mais baixas	O design eficiente do BSV suporta micropagamentos e transações de baixo valor com taxas mínimas, tornando-o ideal para pequenas transações casuais e permitindo novos modelos de negócios.
Eficiência em sistemas de pagamento	As transações do BSV são confirmadas em segundos, tornando-o adequado para transações sensíveis ao tempo sem os atrasos comuns em sistemas bancários tradicionais.
Flexibilidade em casos de uso	O BSV suporta uma variedade de aplicativos além de pagamentos simples, incluindo contratos inteligentes, tokens e operações de dados complexas - tudo em uma camada de blockchain - aumentando sua utilidade enquanto mantém sua eficiência nativa.

Figura 8 - Benefícios da rede BSV.
Fonte: Adaptado de [37].

3.5 Smart Contracts utilizando a rede BSV e o sCrypt

Os Smart Contracts na rede Bitcoin SV são baseados no modelo UTXO, isto é, transações recebidas que não foram gastas, onde cada transação consiste em algumas entradas e saídas.

Uma saída é composta por:

- A quantidade de bitcoins que ele contém;
- Bytecodes, referentes ao script de bloqueio (do inglês, *Locking Script*)

Uma entrada contém:

- Uma referência à saída da transação anterior;

- Bytecodes referentes ao script de desbloqueio (do inglês, *Unlocking Script*)

Um tipo de script de bloqueio é o P2PKH, que verifica se o gastador possui a chave privada correta correspondente ao endereço para que possa produzir uma assinatura válida no script de desbloqueio. O script expressivo permite que o script de bloqueio especifique condições de gastos arbitrariamente mais complexas do que o simples P2PKH, ou seja, fornece a base para a construção dos contratos inteligentes [38].

3.6 Trabalhos Relacionados

Há inúmeros trabalhos que fazem uso de tecnologia Blockchain, provando que é possível utilizá-la em diferentes aplicações. Originalmente a Blockchain foi desenvolvida para a criptomoeda Bitcoin, porém agora conta-se com uma variedade de aplicações em diversos domínios [39]. Nessa seção constam exemplos práticos de aplicações e a Tabela 5, mostra um resumo de alguns trabalhos que fazem uso da tecnologia Blockchain, seja através da construção de contratos inteligentes, ou outras aplicações, visando comparar os trabalhos relacionados e a proposta desenvolvida neste estudo. A fim de evidenciar as diferenças e as vantagens do modelo desenvolvido neste estudo.

Aplicação	Resumo	Comparação com o trabalho desenvolvido	Autor
Aplicação da Blockchain na indústria farmacêutica.	O design proposto integra um aplicativo móvel com a blockchain, onde o fabricante gera os medicamentos e os disponibiliza na blockchain. O modelo executa o contrato que conecta todas as partes interessadas em uma cadeia de suprimentos farmacêutica.	O contrato inteligente desenvolvido também conta com a possibilidade de auditar todas as transações que trafegam na rede, o diferencial é a lógica serial desenvolvida neste trabalho.	[40]
Aplicação da Blockchain na indústria agrícola (BIoT).	O protótipo desenvolvido simula um sistema que rastreia o crescimento das plantas, através da leitura dos dados provenientes dos sensores. O	Assim como no estudo que apresentamos, também foi considerado os aspectos de desempenho do algoritmo em uma blockchain pública. O	[41]

	desempenho do algoritmo foi testado utilizando contratos inteligentes em uma blockchain pública.	foco que demos foi em questões envolvendo escalabilidade, através do uso da rede BSV.	
Acesso e Compartilhamento de Dados de Saúde em Blockchain	Solução que cria contratos inteligentes na rede BSV, para armazenamento, acesso e compartilhamento de dados médicos de pacientes de forma a automatizar o acesso aos seus registros médicos, garantindo confiabilidade através de uma rede imutável e descentralizada.	O contrato inteligente desenvolvido também faz uso da rede BSV, e sua principal vantagem é a possibilidade de envolver e priorizar as demandas empresariais, buscando sanar problemas de vazamento de dados sigilosos.	[42]
Desenvolvimento de uma Micro-Blockchain privada para coleta de dados de dispositivos IIOT	Solução que mostra a blockchain como uma solução eficaz para garantir a integridade e segurança dos dados na Internet das Coisas Industrial (IIoT).	Este trabalho não utiliza uma blockchain privada, e isso se torna uma vantagem para as demandas empresariais de assinaturas de contratos.	[43]

Tabela 5: Comparação de trabalhos envolvendo contratos inteligentes.
Fonte: A autora.

Diante disso, é inegável que a tecnologia Blockchain pode agregar valor as demandas do mundo conectado. Por exemplo, a Blockchain aliada a medicina, fornece muitos meios de desenvolvimento e possibilidades de crescimento para o país. Projetos envolvendo *health care*, processamento de imagens médicas, tratamento de dados provenientes de exames clínicos etc., que fazem uso de Blockchain são realidade em todo mundo, e estudos afirmam que essas aplicações evitam desperdícios [40].

A incorporação da tecnologia da Internet das Coisas (IoT) transformou o mercado atual de diferentes maneiras. O estudo realizado em [41], investiga os benefícios da fusão das tecnologias IoT e Blockchain (*BIoT*) na agricultura, visto que a arquitetura distribuída da blockchain busca resolver as diversas vulnerabilidades que um sistema centralizado fornece, tais como os riscos envolvendo as violações de segurança e o acesso a dados confidenciais de

dispositivos conectados. Esses casos de uso ajudaram na observação e análise do desempenho da plataforma blockchain em relação às métricas de rendimento, latência e escalabilidade.

Dessa forma estes trabalhos destacam questões de eficiência, transparência e segurança como benefícios significativos do uso da tecnologia Blockchain e contemplam também algumas análises envolvendo custos, a fim de mostrar que o sistema, como um todo, é rentável.

CAPÍTULO 4 – ASPECTOS DE SEGURANÇA EM CONTRATOS INTELIGENTES

Há inúmeras aplicações para contratos inteligentes na atualidade. O intuito de criar um modelo de contrato inteligente multiassinatura, possui o objetivo de atender as demandas empresariais de forma segura e transparente. É importante ressaltar que os contratos inteligentes podem contribuir com a segurança dos dados envolvidos nos contratos. Para tanto, fez-se um estudo da Lei n° 13.709/2018 que atualmente rege essa relação de segurança de dados no Brasil.

4.1 A LGPD e a Segurança de Dados

A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei n° 13.709/2018, foi promulgada para proteger os direitos fundamentais de liberdade e de privacidade, e a livre formação da personalidade de cada indivíduo. Essa lei dispõe sobre o tratamento de dados pessoais, dispostos em meio físico ou digital, feito por pessoa física ou jurídica de direito público ou privado, englobando um amplo conjunto de operações que podem ocorrer em meios manuais ou digitais, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural [44].

Embora a autonomia nas relações contratuais privadas seja regra, a inserção de proteções tipicamente destinadas à pessoa natural, em negócios jurídicos empresariais, pode causar confusão e tumultuar relações em que tais direitos não estão tutelados pela lei brasileira de proteção de dados. Isso porque a proteção de informações empresariais pode e deve ser regulada de maneira específica, a exemplo de acordos de confidencialidade ou cláusulas de sigilo e/ou proteção das informações compartilhadas no âmbito da relação contratual negociada entre as partes [45].

A lei em questão oferece tratamento para proteção de dados de crédito, dados pessoais de acesso público, dados pessoais de pessoas sensíveis entre outros, sejam eles compartilhados por conta de relações de trabalho ou consumo. [45]

O principal motivador para o modelo de contrato desenvolvido neste estudo, provém de uma indevida utilização da Lei Geral de Proteção de Dados (LGPD) nos contratos empresariais. Pois apesar de possuir o intuito de proteger as informações pessoais, e buscar a conformidade

com a legislação, há inúmeras empresas utilizando a norma de forma indevida, levando a não proteção dos dados em contratos empresariais [46].

4.2 Ferramentas de Assinatura Digital existentes no mercado

Existem diversas ferramentas para assinatura de documentos/contratos no mercado atual, com diferentes funcionalidades que visam oferecer aos usuários a possibilidade de enviar, assinar e administrar seus contratos. Vale ressaltar que as assinaturas eletrônicas são legalmente reconhecidas no Brasil desde 2001, com a edição da Medida Provisória nº 2.200-2/2001 (MP 2.200-2/2001) que, além de criar a Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil, estabeleceu os critérios de validade das assinaturas eletrônicas no Brasil. Além da MP 2.200-2/2001, outras leis fundamentam a legalidade das assinaturas eletrônicas no Brasil, como o Código Civil, a Lei 13.874/2019 (a Lei da Liberdade Econômica), a Lei 14.063/2021 (assinatura eletrônica envolvendo entes públicos e em questões de saúde pública), a Lei 14.129/2021 (a Lei de Governo Digital), a Lei 14.382/2022 (a Nova Lei dos Cartórios), dentre outras leis e regulamentos [47].

De posse dessas informações, faz-se necessário analisar as ferramentas utilizadas hoje, na maioria das assinaturas dos contratos empresariais, sejam eles de quais tipos forem. Isso é essencial pois os contratos possuem sempre muitas informações relevantes sobre as partes envolvidas. A seguir, descreve-se algumas análises do ponto de vista da segurança dos algoritmos de criptografia, de três das principais ferramentas utilizadas na atualidade, para assinatura de contratos: DocuSign, ClickSign e Assinatura GOV.

De acordo com [47], a plataforma Docusign teve seu início em 2003, sendo uma das pioneiras no desenvolvimento da tecnologia de assinatura eletrônica auxiliando as organizações a se conectarem e automatizarem como preparam, assinam, agem e gerenciam seus contratos.

Um dos aspectos relevantes no que tange a segurança da informação, a Docusign dispõe de criptografia avançada AES (Advanced Encryption Standard) de 128 bits e SSL (Secure Socket Layer) de 256 bits, backups programáveis, acesso à plataforma mediante login e senha, além de camadas adicionais de segurança (como autenticação de dois fatores) [47].

O AES é uma chave simétrica, que se baseia no uso da mesma chave tanto para criptografar quanto para descriptografar os conteúdos. A criptografia cifra e protege as etapas de transferência de dados online [47]. O SSL é responsável por manter os canais de

comunicação criptografados durante a transferência de dados. Funciona a partir de uma chave pública e outra privada, possibilitando a troca segura de informações entre aplicativos e servidor. Para enviar a chave pública, o sistema verifica se o certificado enviado é confiável, válido e se relaciona com o site que o enviou. A mensagem criptografada com chave pública só é decifrada com a inserção da chave privada [47].

O uso da ferramenta é feito da seguinte forma: O usuário recebe por e-mail uma notificação com um link seguro para acesso ao documento. Então, é só analisar e assinar eletronicamente no DocuSign. Para isso, será solicitado que você adote um estilo para sua assinatura ou rubrica, podendo ser: um estilo predefinido do DocuSign, um desenho da sua assinatura ou rubrica ou um upload de uma imagem. Isso é um tanto perigoso, pois uma imagem tende a não refletir fielmente a assinatura do usuário.

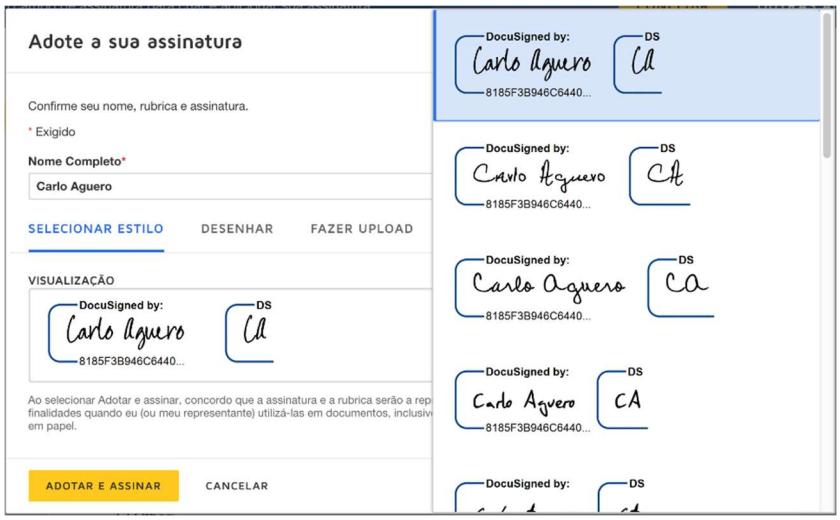
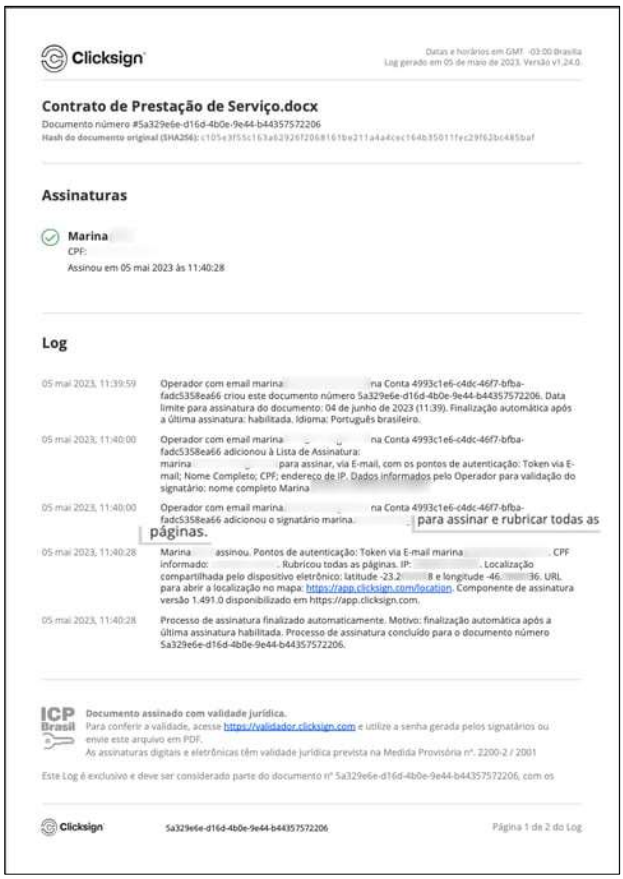


Figura 9 - Possibilidades de assinatura via Docusign.
Fonte: [47].

Por sua vez, conforme [48], a Clicksign foi fundada em 2010, com o objetivo de agilizar processos e trazer mais segurança e eficiência aos procedimentos de assinatura. Com relação a segurança, a Clicksign faz uso do algoritmo de cifra AES-256, e utiliza o Transport Layer Security (TLS) versão mínima 1.2 com validação estendida e criptografia de 256 bits para aumentar a proteção de informações durante a transmissão por redes públicas. O TLS é um protocolo de segurança que garante a integridade de dados entre dois aplicativos de comunicação. Ele tem como objetivo garantir que a conexão entre o navegador, aplicativos e serviços da web seja segura e confiável [48].

Uma funcionalidade que se pode destacar é o log presente nos documentos assinados, pois na Clicksign, existe uma página anexa com o histórico completo das assinaturas. Onde fica

registrado de forma detalhada todo o processo de identificação e responsabilidades dos signatários do documento, com informações como nomes, endereços de IP, e-mails, métodos de autenticação e assinatura e dia e horários em que foram assinados.


Clicksign

Datas e horários em GMT -03:00 Brasília
Log gerado em 05 de maio de 2023. Versão v1.24.0.

Contrato de Prestação de Serviço.docx

Documento número #5a329e6e-d16d-4b0e-9e44-b44357572206

Hash do documento original (SHA256): c105e3f55c163a629267206816 1be211a4a4cec164b35011fec29f63bc485baf

Assinaturas

Marina
CPF:
Assinou em 05 mai 2023 às 11:40:28

Log

05 mai 2023, 11:39:59 Operador com email marina na Conta 4993c1e6-c4dc-46f7-bfba-fadc5358ea66 criou este documento número 5a329e6e-d16d-4b0e-9e44-b44357572206. Data limite para assinatura do documento: 04 de junho de 2023 (11:39). Finalização automática após a última assinatura: habilitada. Idioma: Português brasileiro.

05 mai 2023, 11:40:00 Operador com email marina na Conta 4993c1e6-c4dc-46f7-bfba-fadc5358ea66 adicionou à Lista de Assinatura: marina para assinar, via E-mail, com os pontos de autenticação: Token via E-mail; Nome Completo; CPF; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Marina

05 mai 2023, 11:40:00 Operador com email marina na Conta 4993c1e6-c4dc-46f7-bfba-fadc5358ea66 adicionou o signatário marina para assinar e rubricar todas as páginas.

05 mai 2023, 11:40:28 Marina assinou. Pontos de autenticação: Token via E-mail marina . CPF informado: . Rubricou todas as páginas. IP: . Localização compartilhada pelo dispositivo eletrônico: latitude -23.2 8 e longitude -46. 36. URL para abrir a localização no mapa: https://app.clicksign.com/location. Componente de assinatura versão 1.491.0 disponibilizado em https://app.clicksign.com.

05 mai 2023, 11:40:28 Processo de assinatura finalizado automaticamente. Motivo: finalização automática após a última assinatura habilitada. Processo de assinatura concluído para o documento número 5a329e6e-d16d-4b0e-9e44-b44357572206.

ICP Brasil Documento assinado com validade jurídica.
Para conferir a validade, acesse https://validador.clicksign.com e utilize a senha gerada pelos signatários ou envie este arquivo em PDF.
As assinaturas digitais e eletrônicas têm validade jurídica prevista na Medida Provisória nº. 2200-2 / 2001

Este Log é exclusivo e deve ser considerado parte do documento nº 5a329e6e-d16d-4b0e-9e44-b44357572206, com os

Clicksign 5a329e6e-d16d-4b0e-9e44-b44357572206 Página 1 de 2 do Log

Figura 10- Log de documentos assinados usando a ClickSign.
Fonte: [48].

Ter todos os dados expostos digitalmente é perigoso para os signatários, o que pode gerar vazamento de informações ou compartilhamento inadequado de dados pessoais entre empresas/serviços. Tanto isso é real que está se tornando cada vez mais comum a presença de notícias dos altos índices de vazamentos de dados ou informações pessoais, no Brasil.

Por fim a plataforma de assinatura gov.br, composta pelo Portal de Assinaturas gov.br, pela API de serviços de assinatura eletrônica e um serviço de validação de assinaturas eletrônicas, foi criada com o objetivo de atender à demanda dos cidadãos brasileiros por serviços públicos digitais [49]. O sistema gov assinatura eletrônica permite que você assine um documento em meio digital a partir da sua conta gov.br e além disso provê a integração entre órgãos e entes públicos.

O documento com a assinatura digital tem a mesma validade de um documento com assinatura física e é regulamentado pelo Decreto nº 10.543, de 13/11/2020 (alterado pelo Decreto nº 10.900/2021) [49].

De acordo com [49], essa solução possui alto grau de segurança, com uso de processos criptográficos, totalmente digital e conta com uma solução em nuvem, que eliminou a necessidade de token ou cartão e permite acesso de qualquer dispositivo computacional.

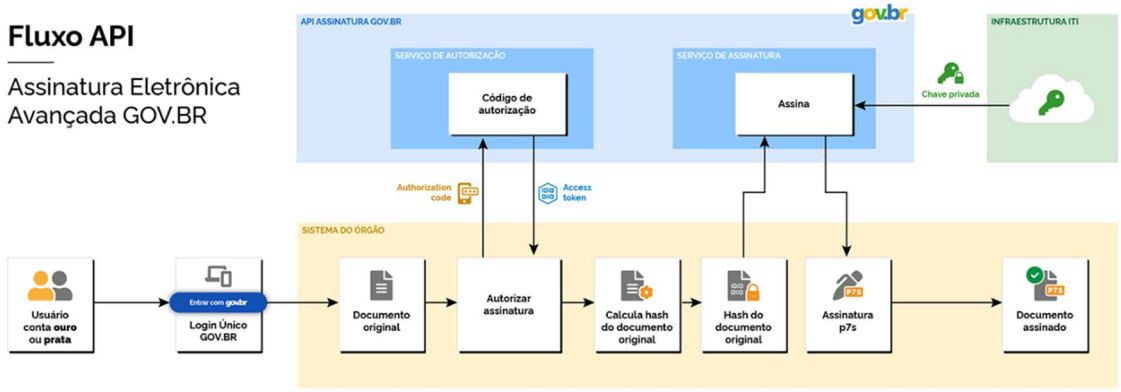


Figura 11 -Fluxo API para assinatura digital gov.br.
Fonte: [49]

Apesar do sistema do e-gov se basear em assinatura digital, a desvantagem se dá no fato de que a chave privada do usuário é controlada por um agente centralizado. E pode-se destacar que os níveis das contas gov: “bronze”, “prata” ou “ouro”, só são atingidos através de mais compartilhamento de dados pessoais, incluindo reconhecimento facial ou validação por internet banking de bancos credenciados. Com isso, o governo garante a identificação de cada cidadão que acessa os serviços digitais.

4.3 Uso de Smart Contracts para assinatura digital

De acordo com [9], em 2022, foram vazados 257 terabytes de dados no mundo, o que corresponde a 2,29 bilhões de informações confidenciais. Desse total, 43% desses vazamentos ocorreram somente no Brasil. O relatório foi feito pela empresa norte-americana Tenable, especialista em gerenciamento de exposição cibernética. Cerca de 35% do total de dados expostos ocorreu devido à desproteção de bancos de dados, demonstrando uma acentuada fragilidade do Brasil no quesito segurança da informação.

Ou seja, as ferramentas de assinatura que dispomos no mercado, podem oferecer riscos quanto a segurança desses dados. Os sistemas de assinatura não são questionados e são utilizados como se fossem 100% seguros.

A ideia proposta nesse estudo é através do uso de *smart contracts* de multiassinatura, tornar possível o uso dessa solução nas assinaturas de contratos empresariais e de qualquer outro fim, na busca de sanar danos à segurança dos dados das partes envolvidas, através do uso de uma forte criptografia proporcionada pela Blockchain.

Consta na Figura 12, um resumo de alguns tipos de criptografia existentes, e também a função *hash*, que segue um caminho alternativo não sendo um tipo de criptografia em si, e sim uma forma de gerar um identificador para um dado, com um resultado único.

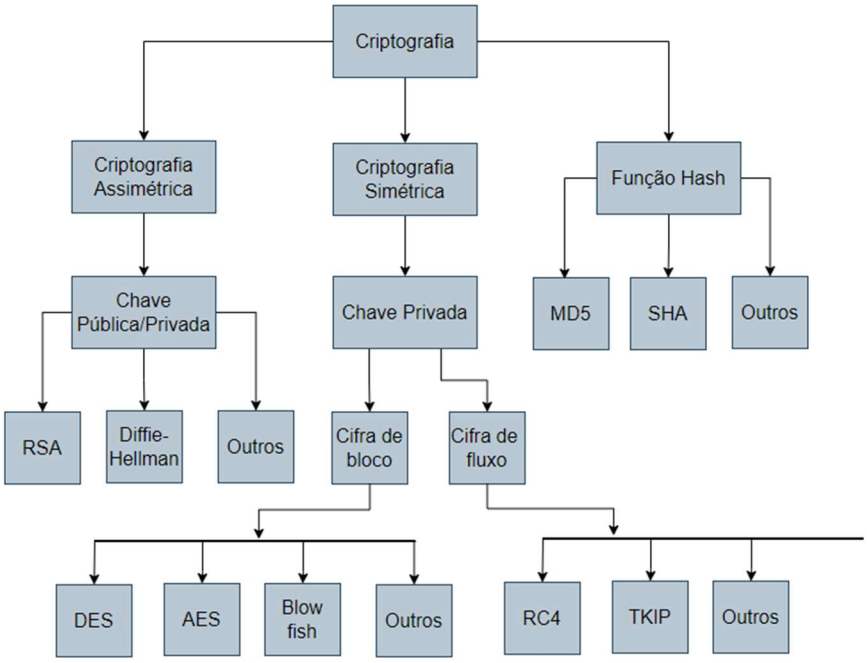


Figura 12 – Tipos de criptografia.
Fonte: Adaptado de [24].

CAPÍTULO 5 – SMART CONTRACT COM MULTIASSINATURA SERIAL

Conforme apresentado na Seção 3.2, esquemas de múltiplas assinaturas podem ser implementados através de contratos inteligente multiassinatura de duas maneiras principais: serial (sequencial) e paralela (concorrente). A escolha entre as opções depende dos requisitos da aplicação ou sistema.

O foco deste estudo se dá na elaboração de um contrato inteligente multiassinatura serial. A principal característica desse tipo de contrato, é que ele não possui a necessidade de aguardar todos os signatários realizarem as assinaturas para que seja validado. Isso é de fato, uma característica inovadora, pois as soluções desenvolvidas em blockchain não contemplam essa possibilidade. O que hoje tem-se implementado na atualidade são esquemas de multiassinatura em paralelo, onde todas as assinaturas são realizadas ao mesmo tempo para que o contrato seja validado na rede.

A construção do modelo desenvolvido, vem da interligação de três arquivos de código: O arquivo do contrato em si, contendo suas regras e particularidades, o arquivo de 'deploy', que permite implantar uma instância de um contrato inteligente na blockchain, e o arquivo de interação do contrato. Os três códigos são unidos entre si para gerar o contrato multiassinatura. A Figura 13 mostra a relação entre o arquivo de regras de contrato, implantação e interação.

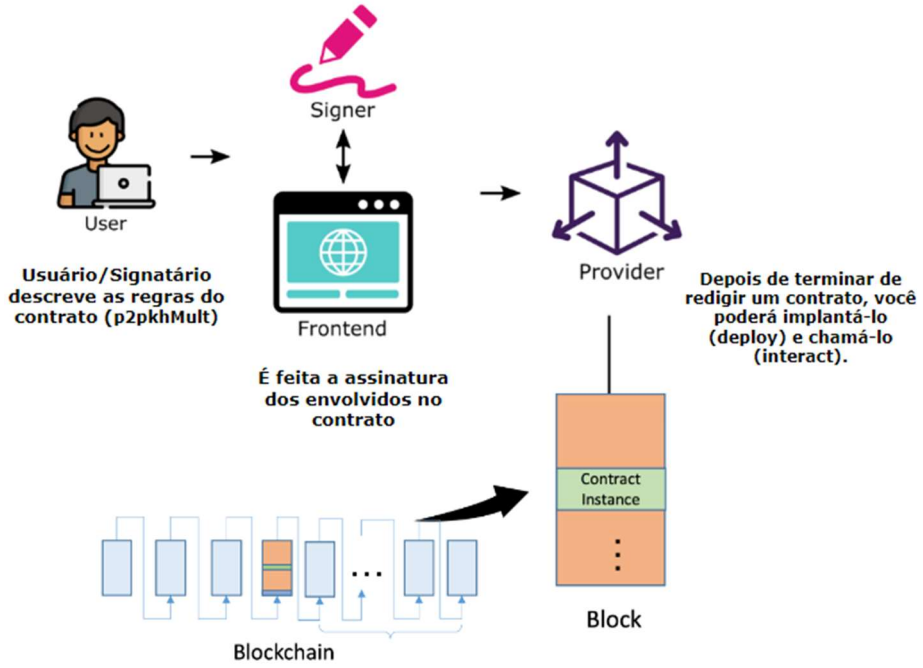


Figura 13 - Relação entre os códigos de regras de contrato, implantação e interação.
Fonte: Adaptado de [19].

Uma das partes mais essenciais na criação de um contrato multiassinatura é o estabelecimento das regras do contrato em si, isto é, as informações pertinentes ao contrato. É necessário entender quem são as partes envolvidas no contrato, bem como a segurança das assinaturas dos envolvidos. Para isso é importante conter no código do contrato a checagem das chaves públicas e assinaturas.

De acordo com [34], um contrato inteligente pertence a classe base *SmartContract*. Os membros da classe chamados @prop e @method serão refletidos na blockchain e, portanto, devem ser um subconjunto estrito ao TypeScript. O modelo construído possui três signatários, os quais possuem chaves únicas e intransferíveis. Dito isso, é necessário que o código entenda quem são e não permita que terceiros assinem o contrato vigente.

A verificação das assinaturas é feita através da função @method e segue a lógica demonstrada na Figura 14:

```
      @method()
      public move(sig: Sig, pbk: PubKey) {

assert((hash160(pbk) == this.sig1) || (hash160(pbk) == this.sig2)
|| (hash160(pbk) == this.sig3), "Bad PublicKey")
        if (hash160(pbk) == this. sig1) {
            assert(this. sig1Sig == false, "Bad signeer")
            this. sig1Sig = true
            this.nSig = this.nSig + 1n
        }
        if (hash160(pbk) == this. sig2) {
            assert(this. sig2Sig == false, "Bad signeer")
            this. sig2Sig = true
            this.nSig = this.nSig + 1n
        }
        if (hash160(pbk) == this. sig3) {
            assert(this. sig3Sig == false, "Bad signeer")
            this. sig3Sig = true
            this.nSig = this.nSig + 1n
        }
        assert(this.checkSig(sig, pbk), "Bad sig")
```

Figura 14- Lógica implementada para verificação de assinaturas.
Fonte: A autora

A lógica implementada para geração do contrato é apresentada na Figura 15, ressaltando as entradas do código, as verificações exigidas e a saída, que são os TX IDs ao final de cada transação.

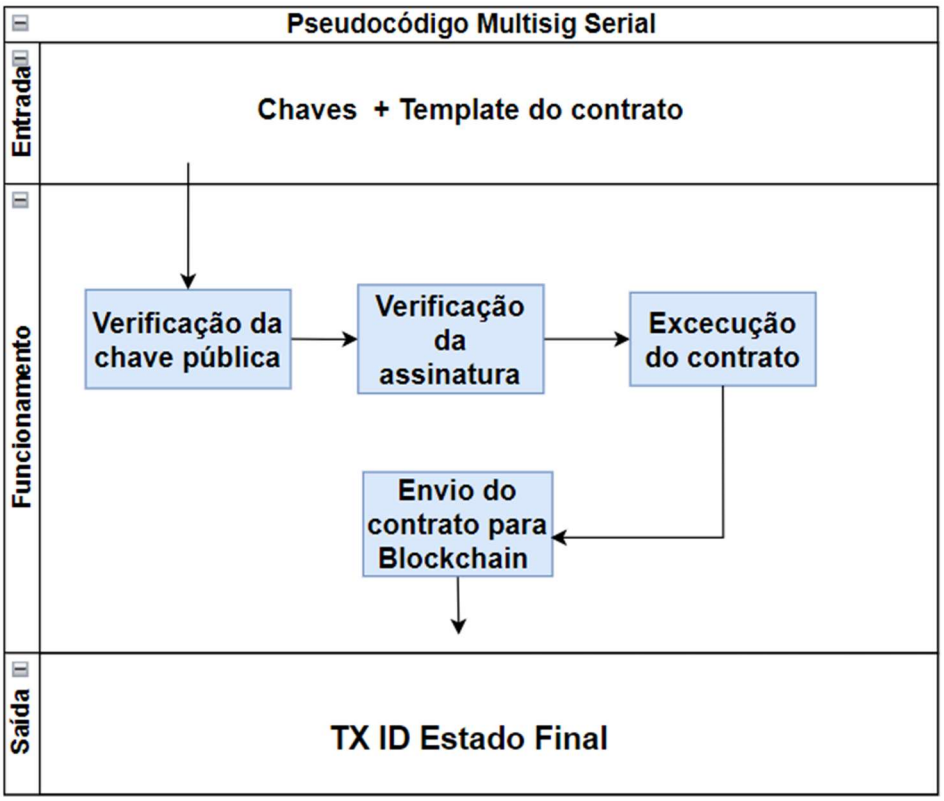


Figura 15 – Lógica implementada no código do contrato multiassinatura serial.
Fonte: A autora.

O contrato inteligente foi gerado na plataforma WEBSV menu, conforme descrito na seção a seguir.

5.1 Interface da plataforma WEBSV menu para Contrato Inteligente

A Websv menu é uma página experimental destinada a apresentar um conjunto de funcionalidades básicas de script Bitcoin que podem ser usadas em diferentes aplicações Blockchain. Através dela é possível realizar uma interação real com a rede Blockchain fazendo uso de uma chave privada em formato hexadecimal. Os recursos do site foram construídos usando a plataforma de desenvolvimento de contratos inteligentes Full Stack Web3 sCrypt-TS [50].

Essa plataforma garante a possibilidade de criar e testar alguns tipos diferentes de contratos inteligentes, e por esse motivo, foi escolhida para a construção do Contrato Inteligente Multiassinatura Serial, proposto nesse trabalho.

O menu principal é dividido em três seções: Home, Satoshi to Peer e Smart Contracts. A interface da plataforma pode ser vista na Figura 16:

Figura 16 – Interface da plataforma Websv menu.
Fonte: A autora.

No menu inicial chamado *Home*, o usuário encontra as funções básicas de acesso para permitir a interação real com a rede blockchain, bem como funções que foram consideradas úteis, tais como: conversão de formato de chave privada, transição da testnet para mainnet, quantidade de satoshis disponível na carteira do usuário e outras funções didáticas adicionais. Ao clicar em *Home*, o usuário é redirecionado para a seção Console de Acesso, onde pode inserir sua chave privada ou senha possibilitando a utilização de todas as funções da página.

No menu *Satoshi to Peer*, o usuário é capaz de realizar algumas das operações mais básicas de blockchain [50]. Esta seção também fornece funções para gravar dados efêmeros na blockchain ou criar tokens de dados básicos, bem como recuperar dados da blockchain. Também existe uma função para recuperar os UTXOs de um endereço ou hash de script.

No menu *Smart Contracts*, o usuário pode criar e testar alguns tipos de contratos inteligentes, tanto contratos sem estado quanto com estado. Na próxima seção, será descrito o processo de geração do contrato em si.

5.2 Contrato Inteligente Multiassinatura Serial

Para o desenvolvimento da interface do contrato inteligente, objeto de estudo desse trabalho, foi criada a aba *Serial Multisignature*. Essa aba foi criada com a finalidade única de gerar os contratos inteligentes de multiassinatura serial, objeto de estudo deste trabalho, conforme mostrado na Figura 17.

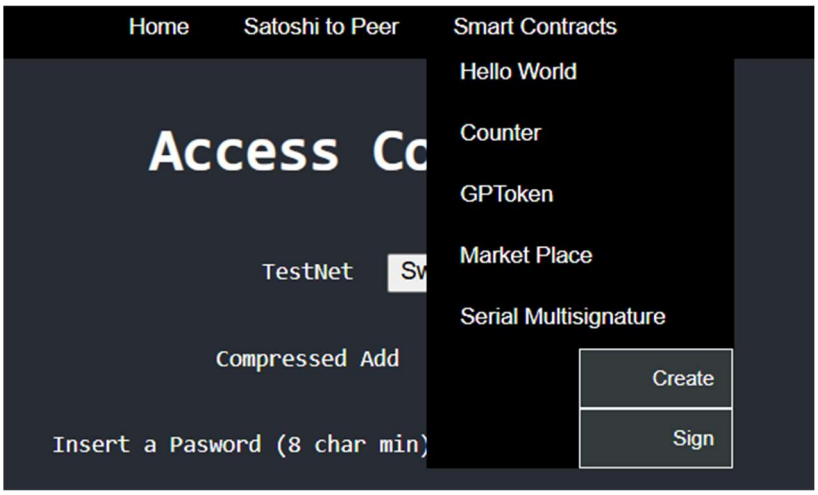


Figura 17 - Aba *Serial Multisignature* desenvolvida para o projeto.
Fonte: A Autora.

É possível observar que o usuário possui a opção de criar um contrato inteligente multiassinatura serial utilizando a aba *Create* e através a aba *Sign* é possível assinar o contrato criado informando o estado do último TX ID da transação. A Figura 18 mostra a interface desenvolvida para a criação do contrato.

Figura 18 – Criação do contrato inteligente através da plataforma Websv.
Fonte: A autora.

De acordo com [51], segundo o Direito Civil brasileiro, um contrato conceitua-se além do acordo de vontades entre duas ou mais partes. É portanto, um acontecimento que repercute na economia e na sociedade, adequando-se aos aspectos formais da lei, e principalmente aos aspectos materiais, tendo como finalidade a igualdade das partes. O contrato tem a finalidade de criar, modificar ou extinguir relação jurídica patrimonial, podendo ser preliminar ou definitivo.

Os elementos essenciais do contrato (res, pretium e consensum) são: o objeto do negócio; o preço convencionado e o acordo das partes, os três requisitos necessários para a construção e conclusão de um contrato [51]. Sendo, portanto, os pilares intrínsecos ao ato, sem os quais não se formaria o negócio jurídico.

Diante do exposto, o contrato criado neste trabalho busca seguir essa linha de raciocínio possuindo o objeto do negócio (quantos signatários precisam assinar), o preço convencionado (satoshis incluídos) e o acordo entre as partes (a assinatura dos envolvidos).

A Figura 19 mostra a interface desenvolvida para assinatura do contrato em si, onde cada signatário, confirma sua assinatura inserindo o último TX ID da transação. O TXID representa um identificador exclusivo atribuído a cada transação na blockchain. A cada

execução de uma transação na blockchain, é gerado um TXID específico. Esse identificador possibilita o rastreamento e a verificação detalhada das transações.

Figura 19- Assinatura do contrato inteligente através da plataforma Websv.
Fonte: A autora.

Esse trabalho é inovador, pois permite utilizar a blockchain no ramo de negócios, e possibilita o uso em diversas aplicações. Tendo em vista as aplicações empresariais, pode-se destacar que essa solução será de grande valia para contratos de compra e venda de ações, bem como contratos de comodato, ou prestação de serviços, por exemplo.

Afinal estes tipos de contratos são utilizados para formalizar a compra ou venda de bens, ou um empréstimo de algo, bem como formalizar os termos de trabalho com clientes. Podendo ressaltar que os termos, preços e condições devem estar detalhados nos contratos.

Na plataforma desenvolvida, o código é totalmente adaptável para essas e outras aplicações, podendo atender as demandas empresariais com clareza e segurança.

5.3 Cenário de testes executados

Os testes foram realizados em vários cenários diferentes, visando garantir a eficácia do modelo proposto:

a) Cenário 1: Ao menos uma das assinaturas corretas é necessária para validação do contrato;
b) Cenário 2: Todas as assinaturas corretas são necessárias para que o contrato seja válido;
c) Cenário 3: Uma assinatura errada, contrato não validado.

Conforme dito anteriormente, uma das vantagens da Blockchain reside no fato de ser uma rede auditável. Portanto é possível rastrear todos os parâmetros das transações estabelecidas dentro da rede blockchain. Para realizar a investigação dos resultados obtidos, foi utilizado a plataforma *WhatsOnChain*, que possibilita o rastreio dos dados em tempo real.

Lançada em novembro de 2018 e adquirido pela Taal Technologies SEZC em setembro de 2020, a *WhatsOnChain* fornece o serviço de explorar a Blockchain BSV em tempo real e serviços de blockchain a nível empresarial [52]. Inicialmente, ela foi concebida apenas como uma maneira de verificar onde as transações estavam no estágio de processamento, então se transformou em uma ferramenta muito útil com infinitas possibilidades, que beneficiam os usuários front-end, e os desenvolvedores back-end [53].

5.3.1 Cenário 1: Ao menos uma das assinaturas é necessária

Para realizar os testes com apenas um signatário, é preciso inserir o número "1" no campo *Number of Signeers*, onde determina-se a quantidade de signatários esperada para este contrato. É importante definir a quantidade de satoshis que serão negociados no contrato e deixar todos os endereços dos envolvidos no contrato disponíveis nos campos *Owner's adresses* conforme mostrado na Figura 20.

As chaves utilizadas nesse projeto são as seguintes:

1) **mtJu3HSiLGobQDJwdQTejHRzebdXFbncBF**
2) **mu8zwsV9f2wVp2fgQUZtpRvyw9WtMob33E**
3) **myR2LCdqKmeNVWJfZ2MtsHt2YYVhkpC1cP**

Figura 20 - Contrato Inteligente Multiassinatura Serial, com apenas uma assinatura.
Fonte: A autora.

É crucial deixar os endereços dos signatários disponíveis, para que o código entenda quem são as pessoas que poderão assinar o contrato, e assim realizar a validação devida. Vale ressaltar que os endereços são informações públicas, o que preserva o sigilo das chaves privadas de cada signatário e não contribui para o vazamento de dados pessoais.

Ao clicar em *Deploy*, o contrato é gerado na rede blockchain, e a interface retorna ao usuário duas informações importantes: o TX ID da transação que envolve este contrato e o link da 'Whatsonchain' referente ao contrato gerado.

Figura 21- TX ID do contrato gerado na rede.
Fonte: A autora.

Ao clicar no link gerado, somos direcionados para a plataforma WhatsonChain, onde é possível checar as informações relacionadas à transação, e todos os detalhes dos dados relacionados a essa transação (data/hora, taxas envolvidas). Também é possível checar de qual bloco essa transação faz parte, e quão grandes são esses blocos. Ou seja, ao utilizar o TXID, o

identificador exclusivo da transação, em qualquer serviço de recuperação disponível na rede, é possível acessar informações específicas sobre a transação.

Figura 22 –Visualização da implementação do contrato na rede blockchain.
Fonte: A autora.

É possível observar as entradas e saídas dessa transação através dos *inputs* e *outputs* gerados, os quais contêm a informação do endereço público, correspondente a chave privada, do signatário que assinou o contrato.

Figura 23 – Entradas e saídas da transação de criação do contrato.
Fonte: A autora.

Após checarmos a existência do contrato na rede faz-se necessário ‘desbloquear’ o contrato, ou seja, assiná-lo, utilizando a aba *Sign* no websv menu. A função implementada nesse

código é responsável por fazer a validação dos ‘outputs’ referentes a transação e checar todas as informações referentes ao contrato em si, garantindo que ele foi executado com sucesso e que as regras de contrato foram estabelecidas.

Para tanto, é necessário incluir o TXID da transação referente ao contrato no campo e clicar em *unlock* :

Figura 24 - Contrato Inteligente assinado e finalizado com sucesso.
Fonte: A Autora.

Após clicar em ‘unlock’ o contrato é finalizado, e a interface retorna ao usuário as informações de TX ID da transação que envolve a finalização do contrato e o link da ‘Whatsonchain’ referente.

Figura 25 - TX ID do contrato finalizado na rede.
Fonte: A autora.

Ao clicar no link gerado, somos direcionados para a plataforma WhatsonChain, onde é possível checar os detalhes da finalização do contrato.

Figura 26 - Visualização da finalização do contrato na rede blockchain.
Fonte: A autora.

É possível observar as entradas e saídas dessa transação através dos *inputs* e *outputs* gerados, os quais contêm a informação do endereço público, correspondente a chave privada, do signatário que assinou o contrato. Dado que a condição para a criação do contrato seria apenas uma assinatura de qualquer um dos três signatários, na finalização do contrato é mostrado qual deles assinou, bem como a data e hora dessa assinatura.

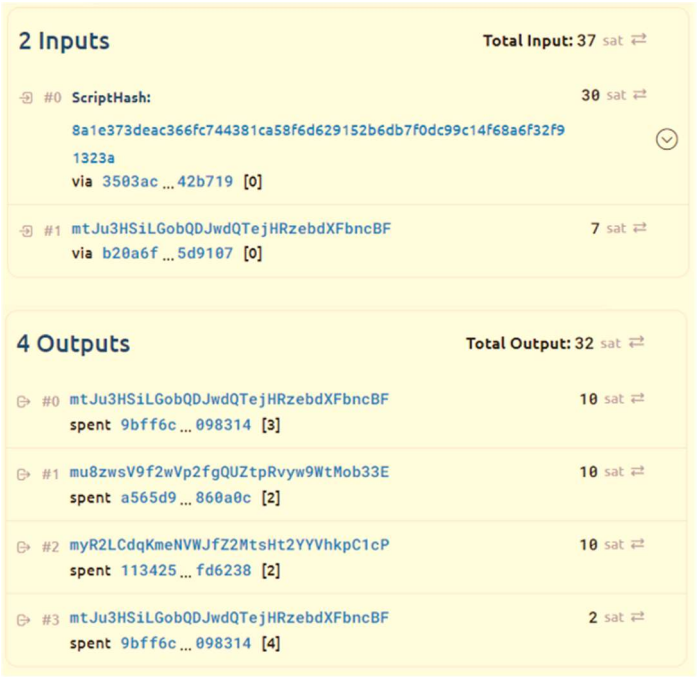


Figura 27- Entradas e saídas da transação de finalização do contrato.
Fonte: A autora.

5.3.2 Cenário 2: Todas as assinaturas são necessárias

Para realizar os testes com todos os signatários, é preciso inserir o número “3” no campo *Number of Signeers*, onde é exigido a quantidade total de signatários esperada para este contrato. É esperado que todos os signatários assinem o contrato, e que todos os endereços inseridos nos campos, correspondam aos signatários.

Figura 28 - Criação do contrato inteligente através da plataforma Websv.
Fonte: A autora

Ao clicar em *Deploy*, o contrato é gerado na rede blockchain. O TX ID da transação que envolve este contrato e o link da ‘Whatsonchain’ referente ao contrato gerado, são fornecidos ao usuário.

Figura 29 - TX ID do contrato gerado na rede.
Fonte: A autora.

Ao clicar no link gerado, somos novamente direcionados para a plataforma WhatsonChain, onde é possível checar as informações relacionadas à transação, e todos os

detalhes dos dados relacionados a essa transação (data/hora, taxas envolvidas). Essas informações são cruciais para a rastreabilidade do contrato.

Figura 30 - Visualização da implementação do contrato na rede blockchain.
Fonte: A autora.

É possível observar as entradas e saídas dessa transação através dos *inputs* e *outputs* gerados, os quais contêm a informação do endereço público, correspondente a chave privada, do signatário que assinou o contrato por primeiro.

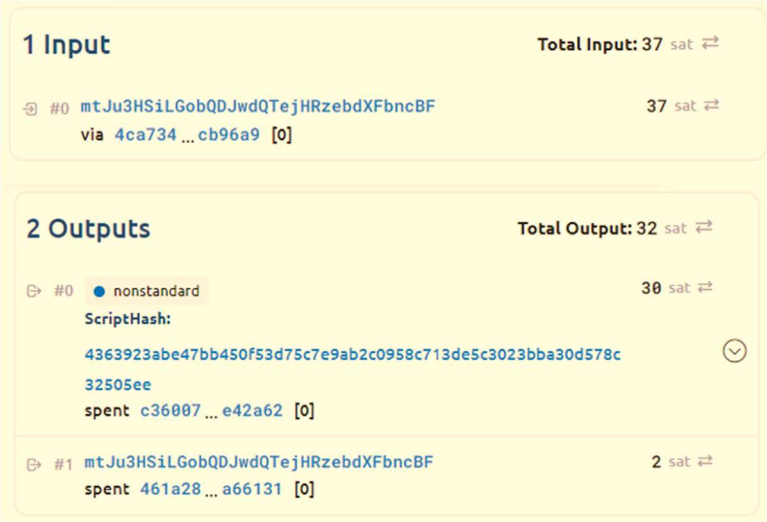


Figura 31 - Entradas e saídas da transação de criação do contrato.
Fonte: A autora.

Após checarmos a existência do contrato na rede faz-se necessário ‘desbloquear’ o contrato, ou seja, assiná-lo utilizando a aba *Sign* construída no *WebSV* menu. A função

implementada nesse código é responsável por fazer a validação dos ‘outputs’ referentes a transação e checar todas as informações referentes ao contrato em si, garantindo que ele foi executado com sucesso e que as regras de contrato foram estabelecidas.

Para continuar o processo de assinatura, o segundo signatário deve logar em ‘Home’ novamente, garantindo que outra pessoa logou na plataforma e quer assinar o contrato. Após isso faz-se necessário resgatar o TXID referente a assinatura anterior e acrescentá-lo no campo exposto e clicar em *unlock* :

Figura 32 - Contrato Inteligente assinado pelo primeiro signatário.
Fonte: A autora.

Figura 33 - TX ID do contrato gerado na rede, após a primeira assinatura.
Fonte: A autora.

Ao clicar no link gerado, é possível checar na Whatsonchain todas as características do contrato, e o mais importante nesse momento é verificar quem assinou e quando assinou, sendo essas informações cruciais para a rastreabilidade do contrato.

Figura 34 - Visualização da implementação da primeira assinatura do contrato.
Fonte: A autora.

Ao enfatizar as entradas e saídas do contrato conseguimos identificar qual endereço realizou a assinatura do contrato.

Figura 35 - Entradas e saídas da transação após primeira assinatura do contrato.
Fonte: A autora.

Para continuar o processo de assinatura, o segundo signatário deve logar em ‘Home’ novamente, para que a plataforma identifique quem está realizando a assinatura. Após isso faz-

se necessário resgatar o TXID referente a assinatura anterior e acrescentá-lo no campo exposto e clicar em *unlock*:

Figura 36 - Contrato Inteligente assinado pelo segundo signatário.
Fonte: A autora.

TXID: 45c65c2ea816634446ed154ba29e91cdd24b2edbb1ae495d91800e499fbb75a2
Link: https://test.whatsonchain.com/tx/45c65c2ea816634446ed154ba29e91cdd24b2edbb1ae495d91800e499fbb75a2

Figura 37 - TX ID do contrato gerado na rede, após a segunda assinatura.
Fonte: A autora.

Ao clicar no link gerado, é possível checar na Whatsonchain os parâmetros da transação. E através da verificação das saídas e entradas é possível detectar quem assinou o contrato.

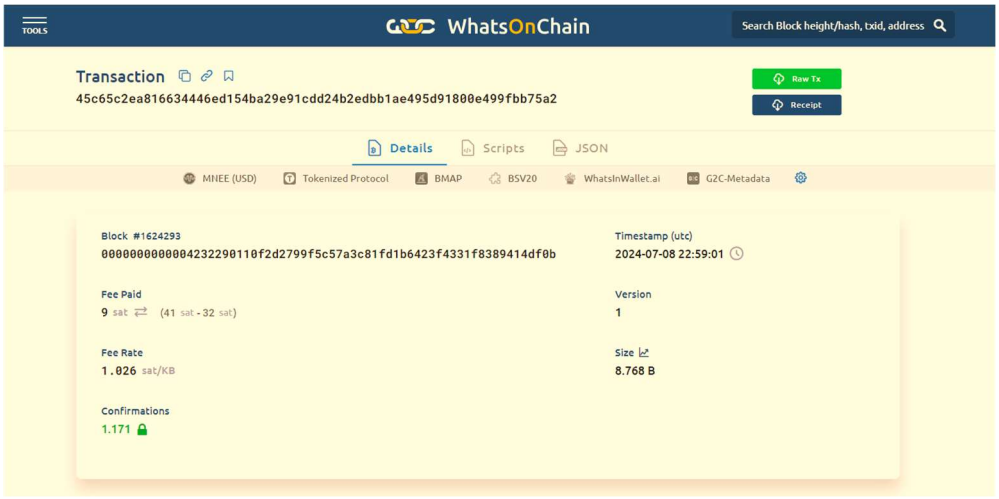


Figura 38 - Visualização da implementação da segunda assinatura do contrato.
Fonte: A autora.

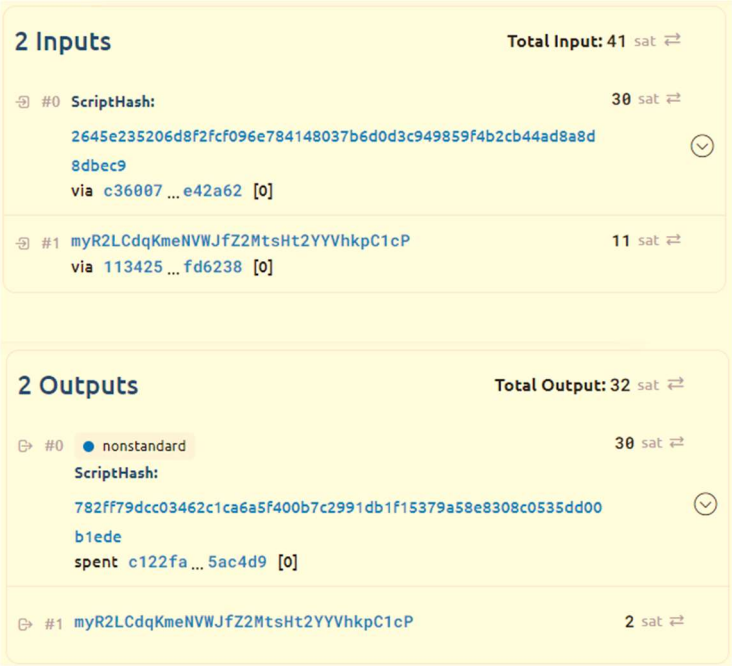


Figura 39 - Entradas e saídas da transação após segunda assinatura do contrato.
Fonte: A autora.

Para finalizar o processo de assinatura, o terceiro signatário deve logar em 'Home' novamente, garantindo a terceira assinatura obrigatória na plataforma. Após isso faz-se necessário resgatar o TXID referente a assinatura anterior e acrescentá-lo no campo exposto e clicar em *unlock* :

Figura 40 - Contrato Inteligente assinado pelo terceiro signatário.
Fonte: A autora.

Figura 41 - TX ID do contrato gerado na rede, após a terceira assinatura.
Fonte: A autora.

Ao clicar no link gerado, é possível checar na Whatsonchain os parâmetros da transação. E através da verificação das entradas e saídas é esperado que seja retornado todos os endereços envolvidos no contrato como saída, demonstrando que todos assinaram antes da finalização do contrato.

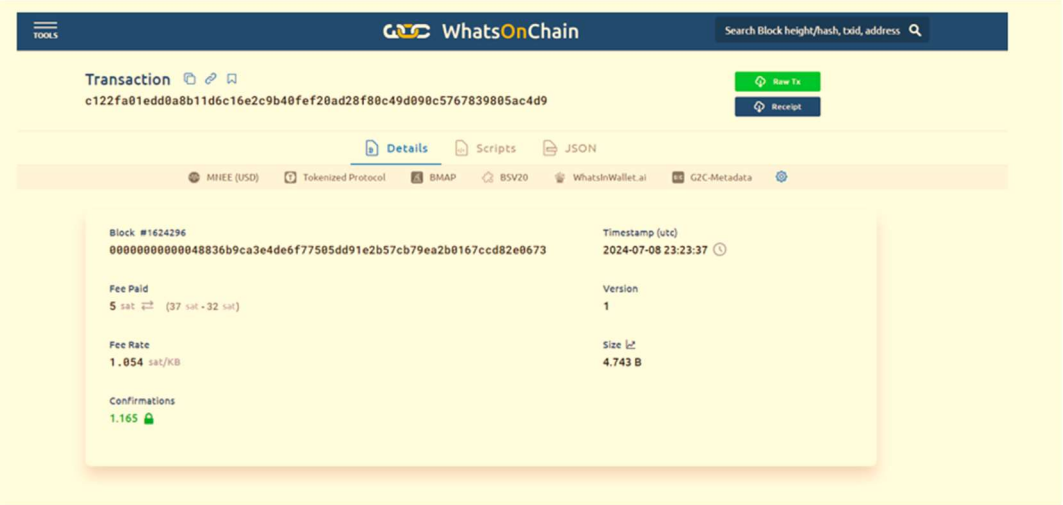


Figura 42 - Visualização da implementação da última assinatura do contrato.
Fonte: A autora.

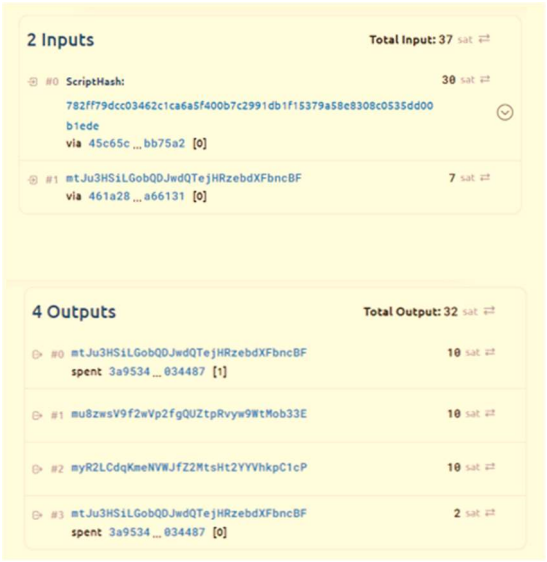


Figura 43 - Entradas e saídas da transação após terceira assinatura do contrato.
Fonte: A autora

5.3.3 Cenário 3: Uma assinatura errada, contrato não validado.

A lógica desenvolvida amarra a validação do contrato à presença dos endereços corretos. A verificação realizada no código é feita através da comparação da chave pública com a assinatura digital. Isso impede que seja adicionado no contrato uma chave pública divergente, ou inexistente. Esse cenário 3 foi idealizado para assegurar que ao inserir um signatário divergente, o contrato não é validado. Portanto, foi criado um contrato, conforme mostrado na Figura 44:

Figura 44- Criação do contrato inteligente através da plataforma Websv.
Fonte: A autora.

Figura 45 - Visualização da implementação do contrato na rede blockchain.
Fonte: A autora.

Figura 46 - Entradas e saídas da transação de criação do contrato.
Fonte: A autora.

É possível observar as entradas e saídas dessa transação através dos *inputs* e *outputs* gerados, os quais contêm a informação do endereço público, correspondente a chave privada, do signatário que iniciou o contrato.

Após isso, apenas para simulação, houve a tentativa de assinatura do contrato utilizando uma chave que não era esperada para esse contrato. A plataforma ao verificar isso, retorna ao usuário a seguinte mensagem:

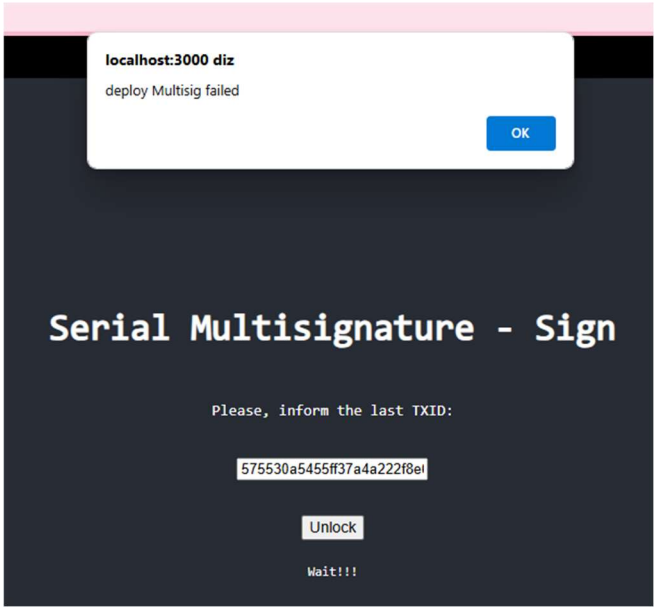


Figura 47 – Contrato não validado, signatário não esperado.
Fonte: A autora.

Então é assegurado que nenhum outro signatário que não seja parte integrante do contrato, tenha poder de assinar o contrato, ou de violá-lo. Isso é de extrema importância no âmbito empresarial, onde trafegam dados sensíveis e confidenciais.

5.4 Resultados e métricas

As características inovadoras do modelo proposto para contratos inteligentes com multiassinatura serial, estão na possibilidade de assinar contratos inteligentes de maneira segura e na adaptação para n signatários. Isso se torna uma solução atraente no ramo de negócios, podendo ser adaptado facilmente a uma rotina empresarial, em diversas áreas e para diferentes fins. Outra grande vantagem é a forma de execução do contrato, pois ao utilizar a lógica serial, o contrato pode ser executado assim que é feita a primeira assinatura, possibilitando que o processo todo seja mais dinâmico.

Este contrato inteligente mostrou um comportamento similar ao que acontece ao usar ferramentas de assinatura digital, oferecidas no mercado atual. Se comparado a um contrato tradicional, o contrato inteligente pode ser mais rápido e econômico. Isso significa que também pode ser incluído como forma de assinatura digital, bem como, pode garantir aspectos de seguranças superiores aos existentes. Além disso, por estar hospedado em uma rede de

blockchain, os acordos não podem ser alterados ou desfeitos. Permanecendo de forma descentralizada e preservando os dados sensíveis das partes envolvidas no contrato.

As assinaturas seriais implicam na possibilidade de auditar a ordem específica em que foram assinadas, isso é vantajoso em situações em que a ordem de aprovação é importante. Para fins de auditoria, por exemplo, observa-se que a natureza sequencial das assinaturas facilita o rastreamento do processo de aprovação.

É possível estabelecer também, uma relação de dependência entre as assinaturas, pois nesse esquema em série, os signatários podem tomar a sua decisão com base nos resultados das assinaturas anteriores, caso queiram. Isso permite aprovações ou rejeições condicionais. Portanto, o contrato elaborado nesse estudo cumpre os objetivos de comprovar a propriedade do contrato e fornecer autorização para gastar os fundos (não repúdio), além de provar que uma transação não foi e não pode ser modificada, e que os dados das partes envolvidas serão protegidos.

Com relação à métricas, pode-se dizer que a escolha da rede Bitcoin SV nos possibilita alcançar resultados importantes, devido ao fato de possuir alta capacidade de processamento de transações, quando comparada a outros modelos de blockchain. Na Tabela 6, tem-se uma comparação de algumas métricas que tornam a rede BSV a maior escolha para essa aplicação:

Aspecto	Bitcoin SV (BSV)	Bitcoin (BTC)	Ethereum (ETH)
Tamanho Máximo do Bloco	Ilimitado	1 MB	N/A (Variável)
Velocidade de Transação	Rápida	Lenta	Rápida
Taxas	Reduzidas	Variável	Variável
Escalabilidade	Alta	Baixa	Alta
Algoritmo de Consenso	PoW (Proof of Work)	PoW (Proof of Work)	PoW (Proof of Work)
Contratos Inteligentes	Sim	Não	Sim
Taxas médias de transação	(11,887 kTPS)	(7 TPS)	(21 TPS)

Tabela 6: Análise comparativa entre os tipos de Blockchain.
Fonte: Adaptado de [43].

Ao assegurar-se a escalabilidade da rede BSV, temos a garantia de que ao usar a rede BSV, as transações serão realizadas eficazmente, pois essa métrica está diretamente ligada a quantidade de transações que esta rede é capaz de processar em um determinado período. Tem-se que o tempo médio de criação de blocos na rede Bitcoin é de cerca de 10 min por bloco, ou seja, a taxa de criação de blocos no tempo tem pequeno impacto na escalabilidade da rede Bitcoin.

Ao analisar o modelo proposto é possível inseri-lo em uma rotina empresarial em contratos de sociedade, compra e venda de ações, comodato, ou de qualquer outro fim, onde todos os envolvidos precisam concordar e assinar para uma tomada de decisão. A abordagem serial fornece um fluxo de trabalho estruturado, que é benéfico em cenários onde se necessita um processo de aprovação claro e linear.

CONCLUSÃO

A proposta deste trabalho foi construir um contrato inteligente multiassinatura serial, evidenciando as diversas possibilidades de uso de contratos inteligentes e sua intrínseca relação com o universo blockchain.

Em linhas gerais pode-se definir a Blockchain como um banco de dados, tratando-se de uma tecnologia que agrupa conjuntos de informações que se conectam por meio de um sistema de hashes que viabiliza o encadeamento seguro e coeso de blocos de informações. Os contratos inteligentes por sua vez, são referidos como contratos digitais que permitem que duas partes assumam alguma forma de troca, tais como: transferência de dinheiro, propriedades e NFTs. Dessa forma, este trabalho demonstrou a importância de entender como os contratos inteligentes são desenvolvidos e suas características, através da explanação de conceitos relevantes, para então implementar o modelo descrito.

Durante a realização desse estudo verificou-se que existem diversas possibilidades de se construir um contrato inteligente, pois para cada aplicação há uma peculiaridade, com objetivos e classificações distintas, de tal sorte que determinar como o contrato será construído, a lógica que será implementada e as regras definidas dependem das necessidades dos signatários.

Este modelo de contrato inteligente possui foco empresarial, diante disso o objetivo principal ao escolher criar um contrato de multiassinatura, é atender as demandas empresariais de forma segura e transparente. O principal motivador para a escolha dessa aplicação provém de uma indevida utilização da LGPD nos contratos empresariais. Mesmo tendo o intuito de proteger as informações pessoais, e buscando a conformidade com a legislação, há inúmeras empresas utilizando a norma de forma indevida, levando a não proteção dos dados em contratos empresariais. Logo, ao propor o contrato objeto de estudo deste trabalho, buscou-se justamente assegurar as boas relações entre contratos e a segurança dos dados dos signatários.

Foram realizados diversos testes para garantir a eficácia do contrato multiassinatura desenvolvido: O cenário 1, exigiu a presença de ao menos uma assinatura, o cenário 2, a necessidade da presença de todas as assinaturas e o cenário 3, mostrou o que acontece caso haja uma assinatura errada. Como resultado disso, todos os cenários foram bem-sucedidos, dentro de seus propósitos. Portanto, é de grande valia salientar que regras de contrato bem-estabelecidas evitam fraudes em contratos e eliminam resultados divergentes.

Dito isso, ao analisar os resultados alcançados por meio dos testes executados, assegura-se que a aplicação desenvolvida possui um impacto relevante nas relações contratuais, podendo gerar inúmeras vantagens para o setor empresarial, ao fazer uso da tecnologia blockchain. Onde pode-se destacar a redução de custos, dos riscos e fraudes, mais transparência e inovação nas relações contratuais, além de aumentar a vantagem competitiva e melhorar a experiência do cliente, tudo isso por meio do uso de contratos inteligentes.

Com relação à métricas, pode-se dizer que a rede Bitcoin SV mostrou capacidade de processamento ideal quando comparada a outros modelos de blockchain. Isso permite atender rotinas empresariais, em contratos de sociedade, compra e venda de ações, ou podemos introduzi-lo em acordos empresariais ou de qualquer outro fim, onde sejam necessárias assinaturas para tomadas de decisão. A abordagem serial fornece um fluxo de trabalho estruturado, que pode ser benéfico em cenários onde é necessário um processo de aprovação claro e linear.

De tal forma que os objetivos gerais e específicos estabelecidos para esse estudo tiveram seus resultados alcançados, além de ter contribuído para um conhecimento mais amplo nos estudos envolvendo essas áreas. Uma análise de possíveis direções para pesquisas futuras e desenvolvimentos na área de contratos inteligentes torna-se cada vez mais necessária no contexto das tecnologias atuais. Como proposta de continuidade desse trabalho, pode ser desenvolvida uma plataforma aberta e pública onde seja possível criar contatos e/ou utilizar para assinatura de contratos. Bem como pode-se realizar adaptações no modelo apresentado ou um estudo comparativo entre contratos inteligentes desenvolvidos na rede BSV e na blockchain Ethereum.

REFERÊNCIAS BIBLIOGRÁFICAS

(1) SOUZA, Rodrigo Couto de. *Tecnologia blockchain na mitigação de vulnerabilidades à corrupção*. 2020. 130 f. Porto Alegre: PUCRS - Biblioteca Digital de Teses e Dissertações.

(2) JAVAID, M., HALEEM, A., SINGH, R. P, Khan, S., SUMAN, R. "*Blockchain technology applications for Industry 4.0: A literature-based review*". Publicado em : Blockchain: Research and Applications, Volume 2, Issue 4, 2021, ISSN 2096-7209, https://doi.org/10.1016/j.bcra.2021.100027.

(3) UPADHYAy, N. "*Demystifying blockchain: A critical analysis of challenges, applications and opportunities*." Publicado em: International Journal of Information Management, Volume 54, 2020, ISSN 0268-4012. https://doi.org/10.1016/j.ijinfomgt.2020.102120.

(4) ALGHAMDI, T. A, et al. "*A Survey of Blockchain Based Systems: Scalability Issues and Solutions, Applications and Future Challenges*," in IEEE Access, vol. 12, pp. 79626-79651, 2024, doi: 10.1109/ACCESS.2024.3408868.

(5) KHALID, M. I. et al., "*A Comprehensive Survey on Blockchain-Based Decentralized Storage Networks*," in IEEE Access, vol. 11, pp. 10995-11015, 2023, doi: 10.1109/ACCESS.2023.3240237.

(6) YANG, W., et al, "*A Survey on Blockchain-Based Internet Service Architecture: Requirements, Challenges, Trends, and Future*". Publicado em: IEEE Access, vol. 7, pp. 75845-75872, 2019, doi: 10.1109/ACCESS.2019.2917562.

(7) AMARO, L. *"Banco Inter testará blockchain para negociação de clientes e transações entre bancos*". Criptofácil, 2023. Disponível em: https://www.criptofacil.com/banco-inter-testara-blockchain-para-negociacao-de-clientes-e-transacoes-entre-bancos/

(8) PARTZ, H. "*Banco Santander testa plataforma blockchain para carros usados no Brasil*". CoinTelegraph, 2022. Disponível em: https://br.cointelegraph.com/news/santander-bank-trials-blockchain-platform-for-used-cars-in-brazil.

(9) FOLHA. "*Quase metade dos dados vazados no mundo são brasileiros, indica estudo*". Disponível em: https://www.folhavitoria.com.br/geral/noticia/05/2023/quase-metade-dos-dados-vazados-no-mundo-sao-brasileiros-indica-estudo. Acesso em: Julho, 2024.

(10) O CONSULTOR JURÍDICO. "*A indevida utilização da LGPD nos contratos empresariais".* 2021. Disponível em: https://www.conjur.com.br/2021-mai-01/zamprogna-indevido-uso-lgpd-contratos-empresariais. Acesso em: Junho, 2024.

(11) BHUTTA, M. N. M. et al., "*A Survey on Blockchain Technology: Evolution, Architecture and Security*". Publicado em: IEEE Access, vol. 9, pp. 61048-61073, 2021, doi: 10.1109/ACCESS.2021.3072849.

(12) NAKAMOTO, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2008. Fonte: Bitcoin Org: https://bitcoin.org/bitcoin.pdf.

(13) ARISTIDOU, Christiana; MARCOU, Evdokia. *Blockchain Standards and Government Applications*. 2019. Publicado em Journal of ICT Standardization, vol. 7, no. 3, pp. 287-312, 2019, doi: 10.13052/jicts2245-800X.736.

(14) SALEH, A. M. S. "*Blockchain for secure and decentralized artificial intelligence in cybersecurity: A comprehensive review*". Blockchain: Research and Applications, Volume 5, Issue 3. 2024. ISSN 2096-7209. Doi: https://doi.org/10.1016/j.bcra.2024.100193. Disponível em: https://www.sciencedirect.com/science/article/pii/S209672092400006X.

(15) DISTRITO NEWSLETTER.*"O que é e como funciona o blockchain: além das criptomoedas".* Disponível em: https://distrito.me/blog/blockchain-o-que-e-como-funciona/. Acesso em: Agosto, 2024.

(16) DASHKEVICH, Natalia; COUNSELL, Steve; DESTEFANIS, Giuseppe. *Blockchain Application for Central Banks: A Systematic Mapping Study*. Publicado em IEEE Access, vol. 8, pp. 139918-139952, 2020, doi: 10.1109/ACCESS.2020.3012295.

(17) NAKAI, T., SAKURAI, A., HIRONAKA, S. and SHUDO, K. "*A Formulation of the Trilemma in Proof of Work Blockchain*". Publicado em: IEEE Access, vol. 12, pp. 80559-80578, 2024, doi: 10.1109/ACCESS.2024.3410025.

(18) COUTINHO, Emanuel F. et al. *Avaliando o Custo de Contratos Inteligentes em Aplicações Blockchain por meio de Ambientes de Simulação*. 2020. Publicado em: Anais do II Workshop em Modelagem e Simulação de Sistemas Intensivos em Software (MSSiS 2020), doi: https://doi.org/10.5753/mssis.2020.12495.

(19) HAFID, A., et al, "*Scaling Blockchains: A Comprehensive Survey*". Disponível em: IEEE Access, vol. 8, pp. 125244-125262, 2020, doi: 10.1109/ACCESS.2020.3007251.

(20) STATISTA, "*Size of the Bitcoin blockchain from January 2009 to June 2, 2024*". Disponível em: https://www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size/. Acesso em: Junho, 2024.

(21) ZHENG, P., et al, "*Blockchain-Based Decentralized Application: A Survey*". Publicado em: IEEE Open Journal of the Computer Society, vol. 4, pp. 121-133, 2023, doi: 10.1109/OJCS.2023.3251854.

(22) SHI, Liucheng. et al, *"Bitmessage Plus: A Blockchain-Based Communication Protocol With High Practicality*". 2021. Publicado em: em IEEE Access, vol. 9, pp. 21618-21626, doi: 10.1109/ACCESS.2021.3056135.

(23) MALAKHOV, A. Marin; ROSSI, Sabina and MENASCHÉ, D. S., "*Confirmed or Dropped? Reliability Analysis of Transactions in PoW Blockchains*," Publicado em: IEEE Transactions on Network Science and Engineering, doi: 10.1109/TNSE.2024.3360080.

(24) DEVAL, V. et al., "Mobile Smart Contracts: Exploring Scalability Challenges and Consensus Mechanisms," in IEEE Access, vol. 12, pp. 34265-34288, 2024, doi: 10.1109/ACCESS.2024.3371901.

(25) Tribunal de Contas da União (TCU). *"Sumário Executivo - Levantamento da Tecnologia Blockchain*". 2020. Disponível em: https://portal.tcu.gov.br/data/files/59/02/40/6E/C4854710A7AE4547E18818A8/Blockchain_sumario_executivo.pdf. Acesso em: Maio, 2024.

(26) SZABO, N. *Formalizing and Securing Relationships on Public Networks*. Publicado em: First Monday Peer-Reviewed Journal of the Internet, (1997). https://doi.org/10.5210/fm.v2i9.548.

(27) GUO. H., YU, X. "*A survey on blockchain technology and its security, Blockchain: Research and Applications*". Volume 3, Issue 2. 2022. ISSN 2096-7209. Doi: https://doi.org/10.1016/j.bcra.2022.100067. Disponível em: https://www.sciencedirect.com/science/article/pii/S2096720922000070.

(28) PORTO, Lucas M. O.; GLÓRIA, Luciano R. T.; BROCHADO, M. "*Contratos Inteligentes na Blockchain: Validade e Restrições".* 2021. Publicado em Revista Teoria Jurídica Contemporânea, vol. 6, doi: 10.21875/tjc.v6i0.44086.

(29) VIDAL, F. R., IVAKI, N., LARANJEIRO, N. "*Vulnerability detection techniques for smart contracts: A systematic literature review"*. Journal of Systems and Software, Volume

217, 2024, 112160, ISSN 0164-1212, Doi: https://doi.org/10.1016/j.jss.2024.112160. Disponível em: https://www.sciencedirect.com/science/article/pii/S016412122400205X.

(30) WU, Z.; XUE, W. and WANG, X., "*Research on Blockchain Smart Contract Optimization for Power Business Scenarios*" 2021. Publicado em: IEEE Conference on Telecommunications, Optics and Computer Science (TOCS), Shenyang, China, 2021, pp. 778-781, doi: 10.1109/TOCS53301.2021.9689013.

(31) YOUSIGN. *Smart Contract: Secure and automate your contractual obligations*. 2023. Disponível em: https://yousign.com/blog/smart-contract#title-14. Acesso em: Junho, 2024.

(32) MEDIUM. *Introduction to Multisig Contracts*: *What is a multisig and which multisig should I use? Here's your answer.* 2020. Disponível em: https://medium.com/mycrypto/introduction-to-multisig-contracts-33d5b25134b2. Acesso em: Junho, 2024.

(33) CANO-BENITO, J.; CIMMINO, A. and GARCÍA-CASTRO*, R. "Toward the Ontological Modeling of Smart Contracts: A Solidity Use Case."* Publicado em: IEEE Access, vol. 9, pp. 140156-140172, 2021, doi: 10.1109/ACCESS.2021.3115577.

(34) SCRYPT. "*Overview sCrypt".* 2023 Disponível em: https://docs.scrypt.io/. Acesso em: Junho, 2024.

(35) BITCOINSV, "*Transactions historical chart*". Disponível em: https://bitinfocharts.com/comparison/transactions-bsv.html#log&3y. Acesso em: Junho, 2024.

(36) COINGEEK CONFERENCE, "*How to achieve green Bitcoin: Energy consumption & environmental sustainability at CoinGeek New York"*. Disponível em: https://coingeek.com/how-to-achieve-green-bitcoin-energy-consumption-environmental-sustainability-at-coingeek-new-york/. Acesso em: Junho, 2024.

(37) BSV BLOCKHAIN. "*The Benefits of BSV Blockchain*". Disponível em: https://docs.bsvblockchain.org/intro/the-benefits-of-bsv-blockchain. Acesso em: Agosto, 2024.

(38) WANG L; et al., "*Smart Contract-Based Agricultural Food Supply Chain Traceability.*" in IEEE Access, vol. 9, pp. 9296-9307, 2021, doi: 10.1109/ACCESS.2021.3050112.

(39) ALZHRANI, F. E., SAEEDI, K. A. and ZHAO, L. "*A Taxonomy for Characterizing Blockchain Systems*". Publicado em: IEEE Access, vol. 10, pp. 110568-110589, 2022, doi: 10.1109/ACCESS.2022.3214837.

(40) SUBRAMANIAN, G; et al., "*Crypto Pharmacy – Digital Medicine: A Mobile Application Integrated With Hybrid Blockchain to Tackle the Issues in Pharma Supply Chain*,"

Publicado em: IEEE Open Journal of the Computer Society, vol. 2, pp. 26-37, 2021, doi: 10.1109/OJCS.2021.3049330.

(41) CHACKO, N. M; et al., "*Exploring IoT-Blockchain Integration in Agriculture: An Experimental Study*" in IEEE Access, vol. 11, pp. 130439-130450, 2023, doi: 10.1109/ACCESS.2023.3334726.

(42) PINHEIRO, T. C. ; et al., "*Acesso e Compartilhamento de Dados de Saúde em Blockchain*." In: XVI Simpósio Brasileiro de Automação Inteligente (SBAI 2023), 2023.

(43) NEVES, J. T., "*Desenvolvimento de uma Micro-Blockchain privada para coleta de dados de ispositivos IIOT*." 2023. PPGGE UFAM: Centro de P&D em Tecnologia Eletrônica da Informação – CETELI.

(44) LEI Nº 13.709 - *Lei Geral de Proteção de Dados Pessoais (LGPD).* 2018. Disponível em: https://www2.camara.leg.br/legin/fed/lei/2018/lei-13709-14-agosto-2018-787077-normaatualizada-pl.pdf. Acesso em: Junho, 2024.

(45) CARLOTO, Selma. "*Lei Geral da Proteção de Dados: Enfoque nas relações de trabalho".* 2ª Edição. São Paulo: LTr Editora, 2021.

(46) O CONSULTOR. "*A indevida utilização da LGPD nos contratos empresariais".* 2021. Disponível em: https://www.conjur.com.br/2021-mai-01/zamprogna-indevido-uso-lgpd-contratos-empresariais. Acesso em: Junho, 2024.

(47) DOCUSIGN. Disponível em: https://www.docusign.com/pt-br. Acesso em: Junho, 2024.

(48) CLICKSIGN, Homepage. Disponível em: . Acesso em: Junho, 2024.

(49) ASSINATURAS ELETRÔNICAS. *"Integração para órgãos e entes públicos"*. Disponível em: https://www.gov.br/governodigital/pt-br/identidade/assinatura-eletronica/assinatura-eletronica-para-orgaos. Acesso em: Junho, 2024.

(50) WEBSVMENU. "*Introduction*". Disponível em: https://medium.com/@cktcracker/websvmenu-faac499d0da5. Acesso em: Junho, 2024.

(51) JUSBRASIL. "*Elementos dos Contratos-Requisitos de Validade*". Disponível em: https://www.jusbrasil.com.br/artigos/elementos-dos-contratos-e-seus-requisitos-de-validade/520405487#:~:text=Os%20elementos%20essenciais%20do%20contrato,e%20conclus%C3%A3o%20de%20um%20contrato. Acesso em: Julho, 2024.

(52) WHATSONCHAIN. "*Explore and build on the BSV Blockchain*". Disponível em: https://whatsonchain.com/about. Acesso em: Junho, 2024.

(53) WHATSONCHAIN REVIEW. “The crypto block explorer all others strive to be”. Disponível em: https://coingeek.com/whatsonchain-review-the-crypto-block-explorer-all-others-strive-to-be/. Acesso em: Junho, 2024.

(54) CRUZ, Carlos. “*Desenvolvimento de Smart Contracts na Rede Bitcoin*”. 2023. OCEAN. PPGGE UFAM: Centro de P&D em Tecnologia Eletrônica da Informação – CETELI.

(55) TRANSAÇÕES BLOCKCHAIN. “*Cenário 1: Ao menos uma das assinaturas corretas é necessária para validação do contrato”.* Disponível em: https://test.whatsonchain.com/tx/3503acb3cf71622cb483e429a3bdc16adc5a55d82b1726c6eae7497ba942b719. Acesso em: Julho, 2024.

(56) TRANSAÇÕES BLOCKCHAIN. “*Cenário 1: Ao menos uma das assinaturas corretas é necessária para validação do contrato*”. Disponível em: https://test.whatsonchain.com/tx/cbbcdbd10f19da6e9d00517cc48f3dc1bfca38eb63b5616d79353c51231d9cae. Acesso em: Julho, 2024.

(57) TRANSAÇÕES BLOCKCHAIN. “*Cenário 2: Todas as assinaturas são necessárias para validação do contrato*”. Disponível em: https://test.whatsonchain.com/tx/58c8cdd385865afcbba5f98b038ad5dc2c9244b7eb0562312f031621a9051046. Acesso em: Julho, 2024.

(58) TRANSAÇÕES BLOCKCHAIN. “*Cenário 2: Todas as assinaturas são necessárias para validação do contrato*”. Disponível em: https://test.whatsonchain.com/tx/c360073c54ed9f285a9416da97c1f43609d5273f93683937f55b7ed589e42a62. Acesso em: Julho, 2024.

(59) TRANSAÇÕES BLOCKCHAIN. “*Cenário 2: Todas as assinaturas são necessárias para validação do contrato*”. Disponível em: https://test.whatsonchain.com/tx/45c65c2ea816634446ed154ba29e91cdd24b2edbb1ae495d91800e499fbb75a2. Acesso em: Julho, 2024.

(60) TRANSAÇÕES BLOCKCHAIN. “*Cenário 2: Todas as assinaturas são necessárias para validação do contrato*”. Disponível em: https://test.whatsonchain.com/tx/c122fa01edd0a8b11d6c16e2c9b40fef20ad28f80c49d090c5767839805ac4d9.

(61) TRANSAÇÕES BLOCKCHAIN. “Cenário 3: Uma assinatura errada”. Disponível em: https://test.whatsonchain.com/tx/575530a5455ff37a4a222f8e6c550fd1a745bfacd97f338c603b6238002df4a3. Acesso em: Agosto, 2024.