Modelo de Autenticação Descentralizada para Chamadas em Smartphones baseada em Credenciais Verificáveis e Blockchain

Jeffson Celeiro Sousa[1], **Antonio Mateus de Sousa**[1], **Sophia Sales**[1], **Bruno Evaristo**[1,2], **Ismael Ávila**[1]

[1] Centro de Pesquisa e Desenvolvimento em Telecomunicações (CPQD)
Campinas – SP – Brasil

{jcsousa, amateus, sophiab, elderb, avila_an}@cpqd.com.br

Resumo. *A digitalização de serviços de telecomunicações traz desafios de confiança, interoperabilidade e proteção de dados que não são plenamente atendidos por modelos centralizados de identidade. Este trabalho propõe um modelo de identidade digital descentralizada baseada em Credenciais Verificáveis e Identificadores Descentralizados para autenticação de entidades em serviços de telefonia, ampliando resultados prévios sobre mitigação de fraudes e caller ID spoofing. A proposta integra blockchain, carteiras digitais e contratos inteligentes em uma visão arquitetural alinhada a padrões internacionais, promovendo um modelo de confiança interoperável, descentralizado e centrado no usuário.*

Abstract. *The digitalization of telecommunications services brings challenges related to trust, interoperability, and data protection that are not fully addressed by centralized identity models. This paper proposes a decentralized identity model based on Verifiable Credentials and Decentralized Identifiers for authenticating entities in telephony services, extending previous results on fraud mitigation and caller ID spoofing prevention. The proposed architecture integrates blockchain, digital wallets, and smart contracts into a unified, standards-aligned framework, promoting an interoperable, decentralized, and user-centric trust model.*

1. Introdução

A crescente digitalização da sociedade, em áreas como mobilidade, administração, saúde, serviços financeiros e cidades inteligentes pode trazer mais eficiência, mas exige cautela. A proteção de dados torna-se crucial à medida que mais e mais usuários expõem dados pessoais em processos digitais online que envolvem coleta, processamento e armazenamento, e cuja conformidade legal é um grande desafio para as empresas. O avanço da digitalização não é mais possível sem uma identidade digital bem definida para os entes que acessam o sistema (por exemplo, cidadãos, autoridades, universidades, empresas públicas e privadas) [Butincu e Alexandrescu 2024].

Nesse contexto, o uso de credenciais verificáveis (VCs) em telecomunicações é promissor em vários casos de uso. Além da garantia da autenticidade das partes originadora e recebedora de uma chamada telefônica, com a verificação automática das respectivas credenciais, o uso de VCs na telefonia tende a trazer mais segurança no uso desse

canal de comunicação, bem como mais interoperabilidade em situações de acesso de dispositivos móveis em *roaming* (itinerância), regional ou internacional [Chen et al. 2021]. Nesse âmbito, o uso de VCs padronizadas permite que essas sejam emitidas, portadas e verificadas de forma descentralizada e interoperável.

Do ponto de vista da gestão de identidades, os modelos tradicionais adotados em serviços digitais e públicos são majoritariamente centralizados, baseados em silos de dados sob controle de provedores de serviço. Embora eficientes sob certos aspectos, esses modelos impõem desafios significativos relacionados à privacidade, transparência e controle pelo usuário final, especialmente em contextos regulados por legislações de proteção de dados, como o Regulamento Geral sobre a Proteção de Dados (GDPR) na União Europeia e a LGPD no Brasil [European Union 2016]. Nesse cenário, os usuários possuem pouca ou nenhuma visibilidade sobre como seus dados são armazenados, processados e compartilhados, o que compromete a confiança nos serviços digitais e amplia a superfície de ataque para usos indevidos ou vazamentos de informações pessoais.

Essa fragilidade do modelo de identidade aparece de forma particularmente crítica nas fraudes telefônicas com falsificação do identificador de chamadas (*caller ID spoofing*) e em chamadas robóticas (*robocalls*). Embora iniciativas regulatórias recentes, como a solução *Origem Verificada* da Anatel, baseada no protocolo STIR/SHAKEN, representem avanços relevantes ao autenticar a operadora de origem da chamada [ANATEL 2025], tais mecanismos não realizam a autenticação criptográfica da entidade originadora. Evidências empíricas internacionais demonstram que essa limitação estrutural permite a continuidade de fraudes, mesmo após a adoção obrigatória do protocolo [TransNexus, Inc. 2022].

Para mitigar as vulnerabilidades de autenticação nos serviços de voz tradicionais, este artigo propõe um modelo de identidade digital descentralizada baseada em VCs e identificadores descentralizados (DIDs), ancorada em uma infraestrutura blockchain. Diferentemente das abordagens que buscam alterar os protocolos de sinalização centrais da rede de telefonia pública comutada (PSTN), as quais precisam acomodar telefones fixos e dispositivos analógicos *offline*, o escopo desta pesquisa concentra-se em um cenário de conectividade moderna. A solução proposta atua como uma camada de sobreposição *out-of-band* voltada especificamente para dispositivos móveis inteligentes (*smartphones*).

Essa abordagem permite que a validação criptográfica da identidade do chamador ocorra de forma paralela ao estabelecimento da chamada de voz nativa, através de um aplicativo cliente. A solução desloca o eixo de confiança da infraestrutura de rede para a identidade verificável das entidades, mitigando fraudes e permitindo interoperabilidade entre domínios administrativos distintos, sem exigir a reestruturação das centrais de comutação legadas.

O restante do artigo está organizado da seguinte forma: a Seção 2 apresenta os trabalhos relacionados; a Seção 3 descreve o modelo proposto; a Seção 4 discute os resultados da prova de conceito; a Subseção 5.1 aborda as limitações e trabalhos futuros; e, por fim, a Seção 5 apresenta as conclusões.

2. Trabalhos Relacionados

Vários trabalhos acadêmicos e iniciativas práticas têm sido propostos para mitigar as chamadas com origem falsa (*caller ID spoofing*) e para estabelecer mecanismos de autenticação em comunicações telefônicas. Wang *et al.* [Wang et al. 2023] propuseram um

mecanismo de *Caller ID Verification* (CIV) baseado em desafio–resposta por tons DTMF, no qual o receptor envia um desafio aleatório ao chamador e valida a identidade comparando a resposta recebida. Embora a abordagem automatize o processo tradicional de *callback* e mantenha a chamada ativa durante a verificação, ela atrasa o estabelecimento, aumenta a carga da rede em cenários de alto volume e oferece proteção limitada, sendo suscetível à interceptação de tons DTMF na ausência de criptografia e assinaturas digitais.

No contexto da PSTN, Tu *et al.* propuseram um esquema de autenticação baseado em infraestrutura de chaves públicas (PKI), no qual uma Autoridade Certificadora (AC) emite certificados de *caller ID* para entes que comprovem a posse do número telefônico [Tu et al. 2017]. Nesse modelo, a central de origem inclui informações estendidas durante o estabelecimento da chamada, permitindo que a central de destino verifique a autenticidade e apresente um indicador de segurança ao usuário final. Apesar de preservar o fluxo unidirecional de sinalização, a proposta exige modificações significativas na infraestrutura das operadoras, impõe maior custo operacional e não garante autenticação ponta a ponta, deixando espaço para interceptação entre usuários finais e suas centrais locais.

Uma variação desse modelo é o registro *RealName*, proposto por Chow *et al.* [Chow et al. 2009], no qual registros jurisdicionais combinam listas públicas de nomes com funções de autoridade certificadora. Instituições registram e monitoram seus identificadores, que são então utilizados na autenticação de chamadas por meio de certificados assinados. Apesar de permitir delegação controlada e cadeias de certificados, o modelo apresenta limitações relevantes, como restrição geográfica, elevada complexidade operacional, múltiplas trocas de mensagens e a necessidade de monitoramento contínuo para evitar conflitos e uso indevido de identificadores.

Li *et al.* [Li et al. 2017] exploraram uma abordagem baseada em terceiros confiáveis, denominada *Trusted Caller ID*, na qual uma autoridade externa valida previamente a associação entre chamador e número telefônico. Durante o estabelecimento da chamada, tanto o emissor quanto o receptor consultam essa autoridade para confirmar a legitimidade do identificador exibido. Embora o modelo dispense alterações diretas na infraestrutura das operadoras, ele introduz latência adicional, cria um ponto único de falha e apresenta limitações de escalabilidade, tornando a autoridade central um alvo potencial para ataques de negação de serviço e campanhas de *robocalls*.

Mais recentemente, abordagens baseadas em blockchain têm sido propostas como alternativas descentralizadas para autenticação de chamadas. Chen *et al.* introduziram o *CallChain*, uma arquitetura que utiliza identificadores descentralizados (DIDs) e credenciais verificáveis (VCs) para autenticar chamadores e destinatários por meio de um canal de dados separado do canal de voz [Chen et al. 2021]. Nesse modelo, os usuários mantêm VCs em carteiras digitais e registram DIDs em um livro-razão distribuído, permitindo autenticação sem dependência de uma autoridade central única. Os autores reportam um acréscimo de aproximadamente 1,6 a 2,1 segundos no tempo de estabelecimento da chamada, considerado aceitável do ponto de vista de usabilidade. Ainda assim, a solução depende de emissores confiáveis para credenciais de número telefônico e seu desempenho está diretamente associado às características da rede blockchain subjacente.

No entanto, embora o *CallChain* ofereça avanços na descentralização, ele atende apenas parcialmente aos requisitos de privacidade e integração móvel, uma vez que a emissão e a gestão de identidades ainda requerem interações complexas que não estão

plenamente encapsuladas de forma transparente para o usuário final de *smartphones*. Ademais, assim como a proposta deste artigo, o *CallChain* restringe-se à necessidade de ter um emissor confiável (como as operadoras de telefonia atuando como *Issuers*), o diferencial da nossa proposta reside na utilização da blockchain exclusivamente para governança administrativa e auditoria, enquanto a verificação das provas criptográficas ocorre totalmente *off-chain* no dispositivo cliente, otimizando o desempenho e a privacidade.

De forma complementar, Liu *et al.* propuseram um esquema para VoIP no qual certificados assinados pelo chamador são ancorados em blockchain após validação por nós autenticadores, sendo posteriormente utilizados para verificar convites SIP [Liu et al. 2020]. Embora essa abordagem elimine servidores centrais dedicados à autenticação, ela mantém dependência de etapas auxiliares de verificação (como SMS) e não aborda diretamente questões de usabilidade ou integração com dispositivos móveis.

No estado da prática, mecanismos amplamente utilizados incluem autenticação baseada em conhecimento, verificação por retorno de chamada (*callback*), aplicativos de identificação de chamadas e sistemas de detecção de anomalias. A autenticação baseada em conhecimento ainda é comum em centrais de atendimento, mas é vulnerável a engenharia social e roubo de dados [Tu et al. 2017]. A verificação por *callback*, embora eficaz em contextos sensíveis, adiciona etapas e pode ser explorada em ataques de *phishing* [Tu et al. 2017]. Aplicativos de identificação de chamadas ampliam a informação exibida ao usuário, mas não garantem autenticidade, e ainda levantam sérias preocupações de privacidade, sobretudo pelo uso de dados de não usuários [Stefanović e Ghilezan 2021]. Por fim, sistemas de detecção de anomalias, adotados por operadoras e reguladores, analisam padrões de tráfego para detectar fraudes, mas não autenticam individualmente o chamador, estando sujeitos a falsos positivos e negativos, sobretudo em ataques sofisticados [1].

Em síntese, embora as abordagens existentes avancem no enfrentamento da falsificação de identificadores de chamadas, elas apresentam limitações estruturais recorrentes. Soluções baseadas em conhecimento, *callback* ou detecção de anomalias não oferecem autenticação criptográfica da identidade do chamador; aplicações de identificação de chamadas carecem de garantias de autenticidade e levantam preocupações de privacidade; e mecanismos regulatórios e de rede, como STIR/SHAKEN, concentram-se na validação da operadora de origem, sem autenticar efetivamente o ente originador da chamada. Por sua vez, propostas acadêmicas baseadas em PKI ou em terceiros introduzem dependências centrais, complexidade operacional ou pontos únicos de falha, enquanto soluções baseadas em blockchain frequentemente demandam elevada participação do usuário ou não exploram plenamente a integração com dispositivos móveis e fluxos reais de chamadas. Dessa forma, permanece a necessidade de uma solução que combine autenticação ponta a ponta do chamador, preservação da privacidade, interoperabilidade entre domínios administrativos e viabilidade de adoção no ecossistema atual de telecomunicações, lacuna que este trabalho busca endereçar por meio do uso de credenciais verificáveis, identidade descentralizada e uma arquitetura blockchain integrada à telefonia móvel.

Como resumido na Tabela 1, a proposta diferencia-se das abordagens anteriores ao integrar autenticação ponta a ponta, IDD de modo viável em dispositivos móveis.

[1] https://kyberturvallisuuskeskus.fi/en/regulations/recommendation-telecommunications-operators-detecting-and-preventing-caller-id-spoofing

Tabela 1. Comparação entre trabalhos relacionados e a proposta apresentada. O símbolo (✓) indica atendimento pleno ao critério (ou resiliência a ponto único de falha); (✗) indica não atendimento; "Parcial"indica suporte limitado.

Abordagem	Autent. Chamador	Autent. Ponta-Ponta	Descentralização	Privacidade Usuário	Ponto Único Falha	Integr. Tel. Móvel
Desafio (DTMF) [Wang et al. 2023]	Parcial	✗	✗	✗	✗	✓
PKI na PSTN [Tu et al. 2017]	✓	✗	✗	Parcial	✗	✓
RealName [Chow et al. 2009]	✓	Parcial	Parcial	Parcial	✗	✗
PCA [Li et al. 2017]	✓	✗	✗	Parcial	✗	✓
Apps Caller ID [Stefanović e Ghilezan 2021]	✗	✗	✗	✗	✗	✓
Blockchain VoIP [Liu et al. 2020]	✓	Parcial	✓	Parcial	✓	✗
CallChain [Chen et al. 2021]	✓	✓	✓	Parcial	✓	Parcial
Proposta	✓	✓	✓	✓	✓	✓

3. Modelo Proposto

Esta seção apresenta o modelo descentralizado proposto, baseado no uso de Credenciais Verificáveis (*Verifiable Credentials* – VCs) associadas a identidades digitais descentralizadas e ancoradas em uma infraestrutura blockchain. O modelo atua como uma camada *out-of-band* voltada para dispositivos móveis (*smartphones*), permitindo a autenticação criptográfica da parte chamadora em paralelo ao estabelecimento da chamada de voz. Isso possibilita que decisões de aceitação ou rejeição de chamadas sejam realizadas de forma automática, verificável e programável nos dispositivos dos usuários, dispensando intermediários centralizados na rede legada de telefonia.

A utilização de VCs mitiga chamadas automatizadas e fraudulentas (*robocalls* e *caller ID spoofing*), uma vez que a aplicação cliente exige a apresentação de uma credencial válida associada ao número originador por um canal de dados, no instante em que a chamada de voz é recebida. No contexto de itinerância (*roaming*) ou acesso a redes 5G, a operadora de origem pode emitir VCs contendo atributos relevantes do assinante (estado de ativação, habilitação para itinerância), favorecendo a portabilidade além-fronteiras sem depender de acordos bilaterais estáticos de sinalização.

3.1. Componentes

O ecossistema do modelo é composto por três elementos principais, cuja interação fundamenta o fluxo de confiança:

- **Carteira Digital (SOUiD):** Aplicativo móvel (desenvolvido com base na arquitetura Bifold em React Native) que atua como o cofre de identidades do usuário. É responsável por armazenar as VCs, monitorar nativamente o estado das chamadas telefônicas no sistema operacional (*ringing*, *off-hook*) e orquestrar a exibição do resultado da validação na tela do dispositivo (interface *overlay*).
- ***Plugin* `did:phone` (Agente ACA-Py):** Um serviço executado sobre agentes ACA-Py (*Aries Cloud Agent Python*) que gerencia o método DID proposto e executa a verificação criptográfica *off-chain* das VCs. Esse componente isola a complexidade criptográfica, permitindo a comunicação via interfaces REST.
- **Blockchain (Hyperledger Indy-Besu [2]):** Atua estritamente como a Infraestrutura de Chaves Públicas Descentralizada (DPKI). Armazena os esquemas (*Schemas*),

[2]https://github.com/hyperledger-indy/indy-besu

definições (*Credential Definitions*), registros de revogação e os DIDs públicos das operadoras (Emissores), mas não armazena dados pessoais dos usuários ou históricos de chamadas.

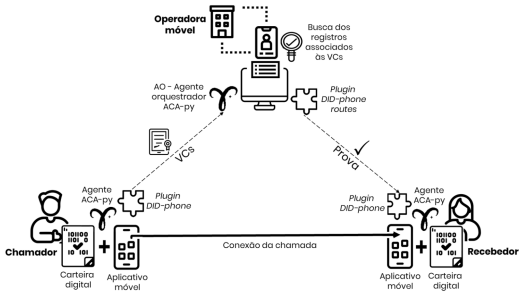

Figura 1. Modelo de solução proposta.

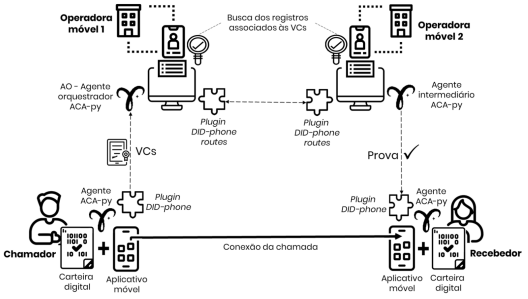

Figura 2. Cenário de chamada envolvendo duas operadoras.

O modelo, ilustrada na Figura 1, utiliza canais DID seguros estabelecidos entre os agentes. Em cenários que envolvem múltiplas operadoras (Figura 2), os agentes orquestradores das respectivas operadoras interagem para fornecer a validação ancorada nas políticas adotadas, suportando a interoperabilidade sem integração direta entre centrais telefônicas.

3.2. Governança do `did:phone` e Prevenção de Falsidade Ideológica

Para garantir que um identificador telefônico E.164 pertença legitimamente à entidade que o reivindica, e para evitar que atores maliciosos registrem números de terceiros (mitigando o *spoofing*), o método `did:phone` opera sob uma governança estrita baseada nas operadoras de telecomunicações.

No modelo proposto, não é permitida a autoemissão (*self-issued*) de credenciais de linha. As operadoras atuam como Emissores Confiáveis (*Trusted Issuers*). Para obter uma VC, o usuário solicita a emissão via SOUiD. A operadora autentica a posse do número (ex: via HSS/HLR ou SMS OTP), assina criptograficamente a VC com sua chave privada e a entrega à carteira do cliente. Se um fraudador tentar gerar um `did:phone` falsificado, a prova criptográfica falhará durante o estabelecimento do canal DID, pois ele não possuirá a assinatura válida de uma operadora reconhecida na DPKI.

3.3. Fluxo de Estabelecimento e Verificação de Chamadas

Para sanar ambiguidades sobre a intermediação da chamada, o modelo distingue dois canais paralelos: o **canal de voz** (roteado via operadora) e o **canal de dados** (verificação P2P via internet).

A sequência de interações (Figura 3) inicia-se quando o dispositivo chamador origina a ligação de voz nativa. O aplicativo SOUiD do recebedor intercepta o evento *ringing* e extrai o *Caller ID*. Imediatamente, via canal de dados, o SOUiD aciona o agente ACA-Py para solicitar (*out-of-band*) uma apresentação de credencial ao agente do originador. O recebedor consulta a blockchain apenas para obter a chave pública da operadora emissora e valida a prova localmente.

Dependendo da validação, o SOUiD exibe no *overlay* as mensagens “Chamada Segura” ou “Chamada Suspeita”. A comunicação assíncrona evita condições de corrida com a rede de voz nativa.

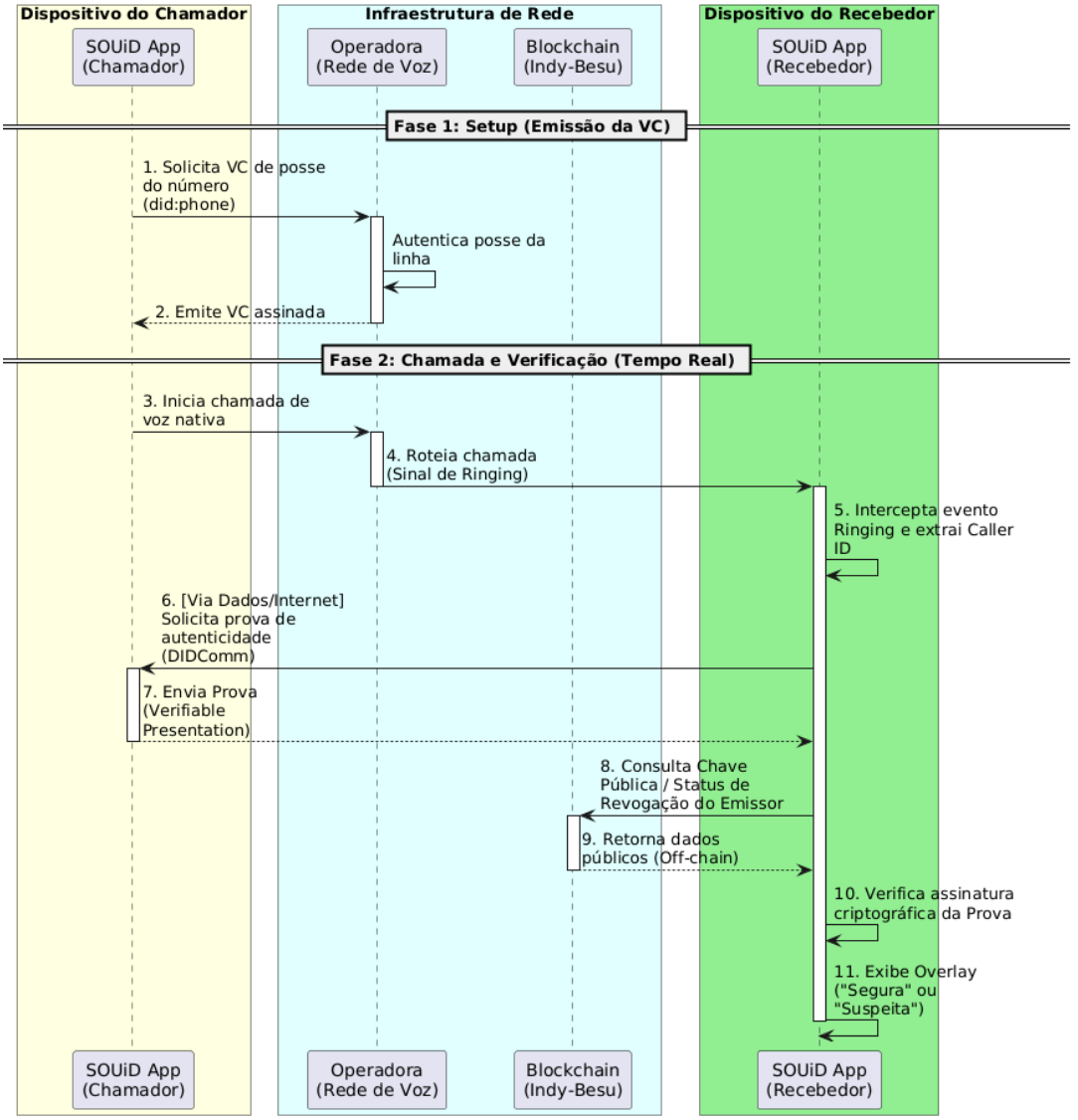

Figura 3. Fluxo de obtenção de credenciais e verificação simultânea à chamada de voz.

4. Resultados e Avaliação

Esta seção apresenta a avaliação da Prova de Conceito (PoC) desenvolvida para validar o modelo proposto. A análise divide-se em três frentes principais: (i) a viabilidade prática da verificação no dispositivo móvel pelo app SOUiD; (ii) o impacto na experiência do usuário (UX) e segurança; e (iii) a avaliação de desempenho dos contratos inteligentes na rede blockchain, validando a escalabilidade do protótipo.

4.1. Avaliação da Aplicação SOUiD

A integração entre o SOUiD e o *plugin* ACA-Py demonstrou a viabilidade da interceptação de chamadas e verificação descentralizada no ecossistema Android.

O Algoritmo 1 evidencia o desacoplamento da solução: o gatilho da verificação é o estado *ringing* (em toque). A partir dele, a requisição é passada ao *plugin* `did:phone` (Algoritmo 2), que busca a conexão, extrai a apresentação da credencial (*Verifiable Pre-*

Algorithm 1 Captura de Eventos de Chamada e Disparo da Verificação (Carteira SOUiD)

Require: Evento de mudança de estado da chamada
Ensure: Disparo condicional da verificação de identidade
1: $state \leftarrow$ GETCALLSTATE()
2: $incoming\_number \leftarrow$ GETINCOMINGNUMBER()
3: **if** $state =$ RINGING **and** $incoming\_number \neq \varnothing$ **then**
4: TRIGGERVERIFICATION($incoming\_number$)
5: **else if** $state \in \{$OFFHOOK, IDLE$\}$ **then**
6: REMOVEOVERLAY()
7: **end if**

Algorithm 2 Verificação da Identidade da Parte Chamadora (*Plugin* `did:phone`)

Require: Número telefônico da parte chamadora ($phone\_number$)
Ensure: $verified \in \{\texttt{true}, \texttt{false}\}$
1: $connection \leftarrow$ QUERYCONNECTION(label = $phone\_number$)
2: **if** $connection = \varnothing$ **then**
3: **return** `false`
4: **end if**
5: $presentation \leftarrow$ QUERYPRESENTATION(connection_id = $connection.id$)
6: **if** $presentation = \varnothing$ **or** $presentation.state \neq$ PRESENTATIONRECEIVED **then**
7: **return** `false`
8: **end if**
9: **if** $verified = \texttt{true}$ **then**
10: **return** `true`
11: **else**
12: **return** `false`
13: **end if**
14: **return** VERIFYPRESENTATION($presentation$)

sentation) e realiza a validação criptográfica. O resultado final é renderizado em um *overlay* na tela do usuário (Figura 4).

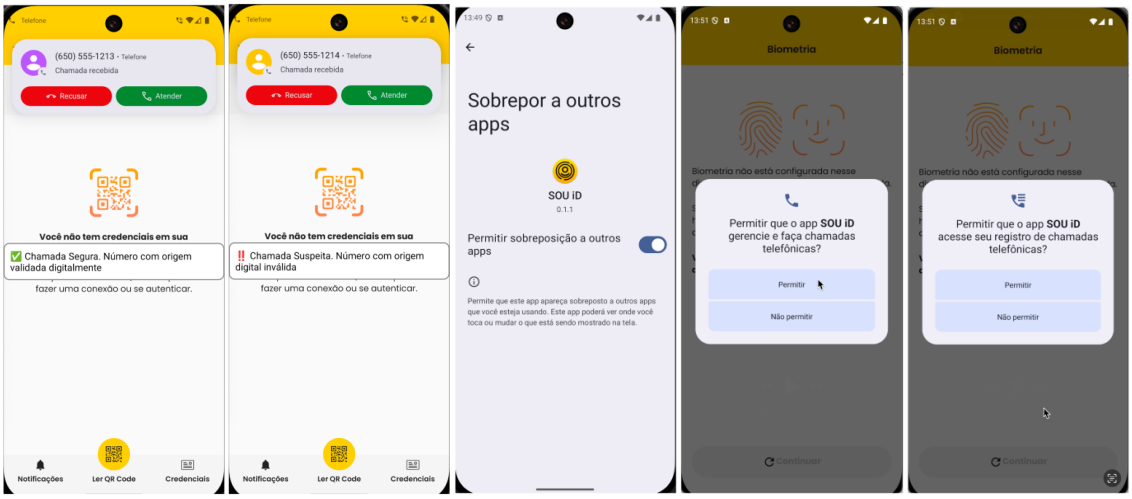

Figura 4. Telas com os resultados da verificação de VCs e de configuração de permissões no SOUiD.

4.2. Experiência do Usuário (UX) e Interface de Feedback

Uma das premissas fundamentais para a adoção de novas camadas de segurança em telecomunicações é a não degradação da experiência do usuário. Como a verificação ocorre em paralelo ao roteamento da chamada de voz, foi necessário implementar um mecanismo de feedback não intrusivo e que respeitasse o tempo de decisão do usuário.

Para esse fim, a carteira SOUiD utiliza um mecanismo de interface sobreposta (overlay), exibido diretamente sobre a tela nativa de chamadas do dispositivo (conforme ilustrado na Figura 4). O overlay é projetado com as seguintes características operacionais validadas na PoC:

- **Independência de Estado:** A mensagem sobre o resultado da verificação ("Chamada Segura"ou "Chamada Suspeita") é exibida independentemente de o aplicativo SOUiD estar aberto em primeiro plano ou de a tela do dispositivo estar bloqueada.
- **Zero Latência Perceptível:** A natureza off-chain da verificação mostrou-se crucial para a UX. Como o aplicativo não submete transações à blockchain durante a ligação, limitando-se a realizar trocas de mensagens DIDComm via internet e verificar assinaturas localmente, os experimentos indicaram que o processo ocorre em frações de segundo. O overlay é renderizado simultaneamente ao tempo padrão de alerta de chamada entrante (ringing delay), permitindo que o usuário tome uma decisão informada antes de atender.
- **Remoção Automática:** A interface informativa é encerrada assim que a chamada transita para os estados off-hook (atendida) ou idle (desligada/rejeitada), minimizando a interferência no uso regular do smartphone.

4.3. Impacto na Segurança e Mitigação de Fraudes

Do ponto de vista qualitativo de segurança, os resultados da PoC indicam uma mudança de paradigma essencial para a rede de telefonia: o deslocamento da confiança. Na telefonia tradicional, a confiança reside no identificador numérico repassado pela sinalização de rede (facilmente manipulável em ataques de spoofing). No modelo proposto, a confiança ancora-se na verificação de uma prova criptográfica emitida por uma entidade regulada (a operadora).

Embora este trabalho não tenha conduzido medições em larga escala sobre a redução percentual de chamadas indesejadas, a implementação comprova que a solução onera assimetricamente o atacante. A automação de campanhas de robocalls ou a prática de falsidade ideológica perdem sua viabilidade econômica e técnica, uma vez que o atacante precisaria comprometer a chave privada da operadora de telecomunicações para gerar uma VC válida para o número falsificado. A ausência de uma credencial válida resulta na imediata categorização da chamada como suspeita pela carteira do recebedor, degradando drasticamente a taxa de sucesso da engenharia social.

4.4. Avaliação de Desempenho dos Contratos Inteligentes

Esta subseção avalia o impacto da camada blockchain no modelo proposto, com foco no desempenho dos contratos inteligentes usados para ancorar políticas de confiança e emissores de credenciais verificáveis. Diferentemente de abordagens que realizam a autenticação *on-chain*, o modelo emprega a blockchain como mecanismo de confiança e auditoria, enquanto a verificação criptográfica ocorre *off-chain*. Assim, a análise concentra-se no custo e na latência das operações necessárias para sustentar esse modelo.

Os resultados de desempenho apresentados nas Figuras 5 e 6 indicam a viabilidade prática do uso de contratos inteligentes de identidade descentralizada como suporte ao *plugin* `did:phone`. A avaliação, conduzida em uma rede Hyperledger Besu com

o auxílio do Hyperledger Caliper, considerou operações típicas do modelo Indy-Besu, como criação de DIDs, esquemas, definições de credenciais e estruturas de revogação, permitindo analisar latência e throughput sob diferentes cargas [3].

Mesmo em cenários de carga elevada, as operações mais custosas, como `createDid` e `createCredentialDefinition`, apresentaram latências compatíveis com processos de provisionamento e registro, os quais não fazem parte do caminho crítico de uma chamada telefônica. Essas funções são executadas tipicamente de forma *offline*, durante o ciclo de vida inicial da identidade do número telefônico, não impactando a experiência do usuário no momento da chamada.

Em contraste, operações mais leves e recorrentes, como `createOrUpdateEntry` e `createRevocationRegistry`, exibiram maior throughput e latência reduzida, mesmo sob cargas mais altas. Esse comportamento é especialmente relevante para o *plugin* `did:phone`, uma vez que a verificação de chamadas depende apenas da validação criptográfica da credencial e da checagem do estado de revogação, ambas realizadas *off-chain*, sem a necessidade de novas transações durante o evento da chamada.

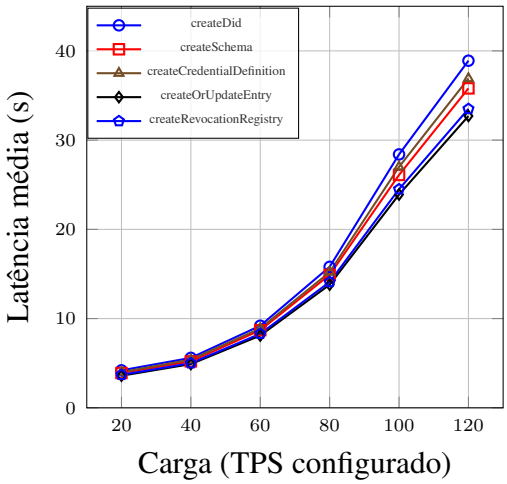

Figura 5. Latência média na rede Besu.

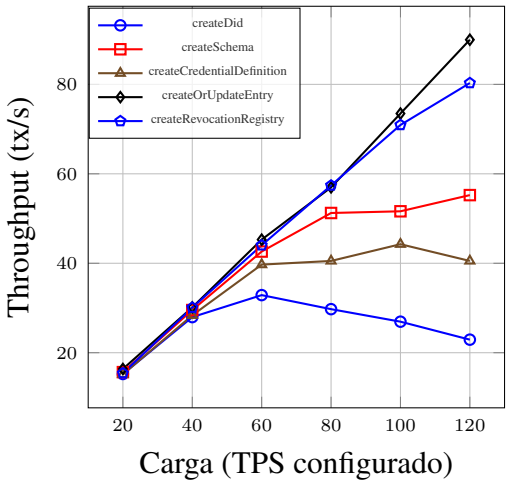

Figura 6. Evolução da vazão / operação.

No modelo proposto, a blockchain é utilizada de forma seletiva ao longo do ciclo de vida das credenciais verificáveis de telefonia. A função `createDid` ancora o número telefônico como um identificador descentralizado (`did:phone:+E.164`), enquanto `createSchema` e `createCredentialDefinition` definem, respectivamente, o modelo de dados e os parâmetros criptográficos da VC. Uma vez emitida, a credencial, contendo atributos como número telefônico, status do assinante, operadora emissora, habilitação para *roaming* e validade temporal, é armazenada na carteira digital do usuário e reutilizada nas verificações, sem a necessidade de novas transações *on-chain* durante o evento da chamada.

As funções `createOrUpdateEntry` e `createRevocationRegistry`, tratam as atualizações e revogações de credenciais, acionadas apenas em situações específicas, como cancelamento de linha ou uso indevido do número. Dessa forma, o custo computacional e a latência da blockchain não impactam o tempo de estabelecimento da chamada, permitindo que a verificação ocorra *off-chain* por meio de validações cripto-

[3] https://github.com/jeffsonsousa/evaluation-contracts-indy-besu

gráficas. Esse desenho desloca o custo para momentos de menor criticidade, preserva a experiência do usuário e torna o *plugin* `did:phone` tecnicamente viável para mitigar *robocalls* e *caller ID spoofing*, além de permitir a aplicação de políticas explícitas e flexíveis de confiança por diferentes domínios administrativos.

Tabela 2. Custo quantitativo de uma credencial verificável de telefonia no contexto do `did:phone`.

Etapa	Funções do Contrato	Frequência	Custo Estimado
Registro da identidade telefônica	`createDid`	Única (setup)	$\sim$ 682k gás ($ $40.93 Ethereum / $0.014 Polygon)
Definição do modelo e parâmetros da VC	`createSchema`, `createCredentialDefinition`	Única (global / por emissor)	$\sim$ 1.13M gás ($ $67.9 Ethereum / $0.023 Polygon)
Uso da credencial em chamadas	Nenhuma (verificação off-chain)	Alta frequência	Zero
Revogação	`createOrUpdateEntry`, `createRevocationRegistry`	Baixa	$\sim$ 150k–300k gás ($ $9–18 Ethereum / $0.01 Polygon)

A Tabela 2 consolida o custo de uma credencial verificável de telefonia ao longo de seu ciclo de vida. Em redes públicas baseadas em EVM, como Ethereum e Polygon, os custos concentram-se nas etapas iniciais de registro e definição criptográfica da identidade. Os resultados indicam que a operação `createDid` consome cerca de 682 mil unidades de gás, valor comparável a registros de domínio *Ethereum Name Service* (ENS) [4]. Em contrapartida, em redes permissionadas ou *gasless*, como a Rede Blockchain Brasil, baseada em Hyperledger Besu com contratos de identidade compatíveis com Indy-Besu [5], esses custos são eliminados ou diluídos, viabilizando a operação contínua do *plugin* `did:phone` em larga escala, sem impacto financeiro direto para usuários finais ou operadoras.

5. Considerações Finais

Este trabalho demonstrou que o uso de credenciais verificáveis e de identidade digital descentralizada em serviços de telefonia móvel constitui uma abordagem tecnicamente viável para mitigar fraudes como *caller ID spoofing* e *robocalls*. Diferentemente de soluções que exigem alterações profundas nos protocolos de sinalização da rede legada (PSTN), a abordagem proposta inova ao estabelecer uma camada de segurança *out-of-band* direcionada a *smartphones*. O modelo validado, materializada pela integração entre a carteira SOUiD, o *plugin* `did:phone` no agente ACA-Py e a rede blockchain Hyperledger Besu, evidenciou a possibilidade de autenticar criptograficamente a origem de uma chamada em tempo real. Ao deslocar a verificação de segurança para o dispositivo cliente (*off-chain*) e ancorar a confiança no registro descentralizado (DPKI), a solução preserva a experiência do usuário, não introduzindo latência perceptível no processo de atendimento.

Os resultados indicam ainda que o modelo de governança, no qual as operadoras atuam como âncoras de confiança na emissão das VCs, amplia a transparência para o recebedor e a interoperabilidade do ecossistema. Em cenários evolutivos, como *roaming* e redes 5G, as VCs reduzem a dependência de acordos bilaterais estáticos de sinalização,

[4] https://etherscan.io/gastracker

[5] https://www.serpro.gov.br/menu/noticias/noticias-2025/serpro-e-blockchain

permitindo que políticas de acesso baseadas em atributos sejam integradas de forma natural aos processos de fatiamento de rede. Assim, o emprego de VCs em telecomunicações afasta a necessidade de intermediários centralizados e estabelece uma base tecnológica escalável para futuras evoluções de segurança e governança nas comunicações unificadas.

5.1. Limitações e Trabalhos Futuros

Apesar da viabilidade comprovada pela PoC, a implementação da solução como um aplicativo de terceiros impõe desafios operacionais que devem ser considerados. Sistemas operacionais móveis modernos, particularmente o Android a partir da versão 15, introduziram restrições de segurança rigorosas que limitam o acesso de aplicativos não nativos a eventos de sistema sensíveis, como o estado contínuo das chamadas. Permissões de monitoramento exigem justificativas explícitas ao usuário e podem expirar ou ser revogadas automaticamente pelo sistema operacional em caso de inatividade. Essa mecânica de restrição de privacidade compromete a capacidade determinística de a solução interceptar o estado *ringing* em tempo real num ambiente de produção de longa duração.

Diante disso, como trabalhos futuros, destaca-se a necessidade de evoluir o modelo para uma integração nativa. A participação direta das operadoras móveis ou de fabricantes de dispositivos (OEMs) permitiria embutir a verificação das VCs diretamente no discador padrão do *smartphone*, utilizando privilégios de operadora. Essa abordagem eliminaria as restrições de permissão em nível de aplicativo e ampliaria a efetividade e a cobertura da solução. Adicionalmente, planeja-se investigar o impacto do protocolo DIDComm no consumo de bateria e dados do dispositivo móvel em cenários de alta volumetria de chamadas, bem como a formalização matemática das provas de segurança da governança do método `did:phone`.

6. Agradecimentos

Os autores agradecem o apoio dado a este trabalho pelo MCTI-Ministério da Ciência, Tecnologia e Inovação, com recursos financeiros do FUNTTEL e administrados pela FINEP, no âmbito especificamente do projeto TEDESCON - **Te**cnologias **De**scentralizadas para **Con**fiança na internet, Contrato 01.25.0761.00, Referência 11117/25.

Referências

ANATEL (2025). Autenticação e identificação de chamadas. `https://www.gov.br/anatel/pt-br/regulado/acompanhamento-e-controle/autenticacao-e-identificacao-de-chamadas`. Agência Nacional de Telecomunicações (ANATEL). Accessed: 2026-01.

Butincu, C. N. and Alexandrescu, A. (2024). Design aspects of decentralized identifiers and self-sovereign identity systems. *IEEE Access*, 12:60928–60942.

Chen, Y., Wang, Y., Wang, Y., Li, M., Dong, G., and Liu, C. (2021). Callchain: Identity authentication based on blockchain for telephony networks. In *2021 IEEE 24th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*, pages 416–421.

Chow, S. T., Gustave, C., and Vinokurov, D. (2009). Authenticating displayed names in telephony. *Bell Labs Technical Journal*, 14(1):267–282.

European Union (2016). General data protection regulation (GDPR). `https://gdpr.eu/`. Regulation (EU) 2016/679.

Li, J., Faria, F., Chen, J., and Liang, D. (2017). A mechanism to authenticate caller id. In Rocha, Á., Correia, A. M., Adeli, H., Reis, L. P., and Costanzo, S., editors, *Recent Advances in Information Systems and Technologies*, pages 745–753, Cham. Springer International Publishing.

Liu, F., Yang, B., Su, L., Wang, K., and Yan, J. (2020). A blockchain based scheme for authentic telephone identity. In Zheng, Z., Dai, H.-N., Fu, X., and Chen, B., editors, *Blockchain and Trustworthy Systems*, pages 675–682, Singapore. Springer Singapore.

Stefanović, T. and Ghilezan, S. (2021). Preserving privacy in caller id applications. In Friedewald, M., Schiffner, S., and Krenn, S., editors, *Privacy and Identity Management*, pages 151–168, Cham. Springer International Publishing.

TransNexus, Inc. (2022). Robocalls up sharply in october 2022. `https://transnexus.com/blog/2022/robocalls-up-sharply-october/`. Accessed: 2026-01.

Tu, H., Doupe, A., Zhao, Z., and Ahn, G.-J. (2017). Toward standardization of authenticated caller id transmission. *IEEE Communications Standards Magazine*, 1(3):30–36.

Wang, S., Delavar, M., Azad, M. A., Nabizadeh, F., Smith, S., and Hao, F. (2023). Spoofing against spoofing: Towards caller id verification in heterogeneous telecommunication systems.