ToID: Reputação Baseada em Identificadores Descentralizados Para Aplicações Distribuídas

Antonio M. de Sousa[1], **Allan E. S. Freitas**[2], **Leobino N. Sampaio**[1]

[1] Departamento de Ciência da Computação – Universidade Federal da Bahia (UFBA)
Salvador – BA – Brasil

[2]Departamento de Computação – Instituto Federal da Bahia (IFBA)
Salvador – BA – Brasil

antonio.mateus@ufba.br, leobino@ufba.br, allan@ifba.edu.br

Abstract. *Reputation systems become an important trust mechanism as the Internet becomes even more decentralized. However, current reputation systems are built on centralized management infrastructures that directly impact privacy and the very decentralization of the network. On the other hand, decentralized reputation models ensure greater scalability and elasticity of applications but sacrifice privacy in favor of participant authenticity. In this work, Trust over IDentity is proposed, aiming to provide a reputation infrastructure based on the decentralized digital identity paradigm to ensure trust without compromising the privacy and authenticity of both service providers and consumers. The proposal was implemented and evaluated through emulations that confirmed its potential in maintaining the integrity of reputation and the possibility of expansion to other application scenarios through the use of smart contracts.*

Resumo. *Os sistemas de reputação se tornam um mecanismo de confiança importante à medida em que a Internet se torna cada vez mais descentralizada. Todavia, os sistemas de reputações atuais são construídos sobre infraestruturas centralizadas de gerenciamento que impactam diretamente na privacidade e na própria descentralização da rede. Por outro lado, os modelos descentralizados de reputação garantem maior escalabilidade e elasticidade das aplicações, mas sacrificam a privacidade em prol da autenticidade dos participantes. Neste trabalho é proposta a Trust over IDentity que visa prover uma infraestrutura de reputação baseada no paradigma de identidade digital descentralizada para garantia de confiança sem afligir a privacidade e autenticidade de ambos provedores e consumidores de serviços. A proposta foi implementada e avaliada através de emulações que confirmaram seu potencial na manutenção da integridade da reputação e possibilidade expansão para outros cenários de aplicações por meio do uso de smart-contracts.*

1. Introdução

Os modelos de confiança convencionais da Internet baseiam-se, predominantemente, no uso de infraestruturas de chaves públicas (PKIs) para garantir a autenticidade das entidades detentoras de credenciais emitidas por suas instituições. A expansão e interoperabilidade das aplicações atuais da Internet têm exigido a adoção de modelos de confiança que, além da autenticidade, permitam qualificar os provedores de serviços. Esta questão tem

sido endereçada através da reputação de entidades, compatíveis com os princípios fundamentais da *Web of Trust* (WoT) [Zimmermann 1992, Caronni 2000, Bellini et al. 2020]. A WoT define-se como uma teia de percepções de reputação entre os pares, que possibilita a tomada de decisão quanto a confiança em redes com múltiplos provedores de serviços e clientes não-confiáveis. Através da reputação é possível quantificar o nível de confiança de uma determinada entidade (e.g., provedor ou cliente) com base no seu histórico de ações [Feraudo et al. 2024].

Na literatura atual, existem diversas propostas que buscam o provimento de serviços de reputação através de duas abordagens principais. A primeira se baseia na gestão centralizada em uma terceira parte confiável, que controla a entrada e remoção de nós, bem como ajuste do cálculo das reputações [Fernandes et al. 2023, Hou et al. 2023]. Apesar de facilitar a gestão dos dados de reputação, a centralização representa um ponto único de falha e pode levar a desafios de escalabilidade. A segunda abordagem consiste na descentralização alcançada através de infraestruturas com controle e mecanismos de consenso distribuídos que mantêm o controle sobre alterações na reputação de uma dada entidade [Feraudo et al. 2024]. Contudo, o tradicional gerenciamento de chave pública (PKI) [Almasoud et al. 2020, Singh et al. 2020, Bellini et al. 2020, Gupta et al. 2003], implica em uma natural centralidade de papel que permite a nós maliciosos tentar comprometer o sistema por ataques focados em uma única entidade.

Este trabalho, portanto, tem como principal objetivo, responder como implementar serviços de reputação distribuídos baseados no gerenciamento também distribuído de identidades e sem comprometer a privacidade dos usuários. Para isso, propomos um mecanismo de reputação baseado no uso de Identidade Digital Descentralizada (IDD) [Avellaneda et al. 2019, Tan et al. 2023]. IDDs possibilitam o gerenciamento de identidades de forma distribuída, em geral através de Tecnologias de *Ledgers* Distribuídos (DLTs). Assim, por meio da IDD, os dados privados (incluindo as próprias credenciais) de uma entidade são armazenados e controlados pela própria entidade, em vez de serem mantidos por terceiros. Nossa solução, denominada por *Trust over IDentity* (ToID), visa prover um mecanismo de reputação que utiliza a IDD de modo a tratar a confiança de fornecedores de serviços na web. Além do uso de IDDs para construir um serviço de reputação, introduzimos o conceito de infraestrutura pública de confiança (do inglês, *Public Trust infrastructure* – PTI).

A ToID foi implementada utilizando contratos inteligentes (do inglês, *smart-contracts*) para a persistência e manutenção da reputação, e uma versão personalizada de agentes gerenciadores de Identidades Digitais Descentralizadas (IDD), como os Aries CloudAgents [Aries 2023], adaptados para integrar-se à arquitetura de Redes de Dados Nomeados (do inglês, *Named Data Networking*)˜[Zhang et al. 2014]. Os resultados experimentais demonstraram os benefícios dos serviços de reputação por meio de uma prova de conceito envolvendo a aplicação de funções nomeadas nas Redes de Dados Nomeados. A análise do algoritmo de reputação proposto mostrou sua eficácia em punir nós que se comportam de maneira inadequada, mantendo a reputação abaixo de 40% nesses casos. Além disso, a ToID mitiga os principais ataques à reputação com sua abordagem descentralizada e centrada no usuário.

O presente artigo está organizado da seguinte forma: na Seção 2, apresentamos uma discussão sobre trabalhos correlatos. A Seção 3 apresenta nossa proposta, cuja

implementação é detalhada na Seção 4. De forma preliminar, exercitamos em uma prova de conceito na Seção 5. Por fim, apresentamos nossas considerações finais na Seção 6.

2. Trabalhos Relacionados

Em [Hou et al. 2023], é proposto um mecanismo de reputação para redes veiculares baseado em uso de duas redes blockchain. A proposta se utiliza de uma inferência bayesiana aprimorada para derivação da reputação com base no histórico de contribuições dos veículos na rede.

Em [Fernandes et al. 2023], os autores avaliaram a autenticidade e racionalidade dos avisos locais de perigo com base na reputação dos veículos. A proposta é implementada sobre uma blockchain com consenso usando PoA (*Proof of Authority*) e avalia por simulação a sobrecusto desta blockchain. Ao atender aos requisitos de eficácia e latência, o esquema proposto pode resistir a ataques de injeção falsa. A premissa da proposta é otimista, ou seja, os nós são inicialmente considerados confiáveis, portanto, quase não há medidas defensivas antes de cometer comportamentos inadequados. Assim, a segurança deste esquema ainda precisa ser testada em aplicações práticas.

Já em [Feraudo et al. 2024], os autores propõem uma solução de reputação também voltada para VANETs, porém integrando o universo de identidade descentralizada como infraestrutura de segurança. Apesar de ser um trabalho inovador, os autores não demonstram como a implementação baseada em identificadores descentralizados (DIDs) foi feita, uma vez que o trabalho aprofunda na capacidade de detecção de falsas informações por meio do mecanismo de reputação.

Os trabalhos de [Hou et al. 2023] e [Fernandes et al. 2023] propõem sistemas de reputação baseados em modelos de identidade centralizados, semelhantes ao mecanismo convencional de PKI. Contudo, apesar desse aspecto centralizado, ambos utilizam mecanismos de livro-razão distribuído por meio de blockchain como suporte descentralizado para a informação de reputação. Por outro lado, a ToID busca prover uma estratégia segura para a implantação de sistemas de reputação, independente do tipo de aplicação, baseada em identidade digital descentralizada, utilizando DIDs fundamentados em um esquema de nomeação proposto e *smart contracts* que suportam a sua utilização.

3. *Trust over IDentity*: reputação baseada em identificadores descentralizados

Trust over IDentity (ToID) é um mecanismo de reputação baseado em identificadores descentralizados (DIDs, do inglês *digital identifiers*) que objetiva prover uma camada adicional de confiança para a Internet. ToID faz uso dos DIDs como alicerce na criação de uma solução robusta e descentralizada de confiança. As características intrínsecas aos DIDs permitem que uma proposta de camada adicional de segurança baseada em reputação seja implementada com sucesso. Algumas dessas características são:

- naturalmente descentralizados e independem de infraestrutura para funcionar;
- escaláveis se utilizados juntamente com livro-razão distribuído ou quaisquer sistema de armazenamento distribuído (e.g. IPFS);
- globalmente verificáveis, isto é, as informações necessárias para validar a identidade do detentor do DID estão disponíveis publicamente (e.g. em uma DLT);
- os chamados *did methods* são ferramentas que favorecem a criação de novos métodos para múltiplos propósitos e enriquecem a semântica dos dados, como por exemplo um *did method* exclusivo para IoT ou um focado em NDN; e

- se gerados corretamente, os DIDs são identificadores únicos e, portanto, identificam apenas uma e somente uma entidade.

Como descrito nas subseções seguintes, ToID observa as características acima para criar uma abordagem que segue os princípios da WoT, propiciando um cenário de confiança distribuída e gerenciada pela própria rede.

3.1. Reputação baseada em DID

ToID se baseia no conceito de *Web of Trust* para manter um grafo que expressa as percepções de confiança existentes entre os nós. Uma questão pode emergir, como implementar a percepção de confiança em um cenário desafiador e inerentemente não-confiável como a Internet? A confiança pode ser percebida por delegação, ou seja, uma entidade na Internet pode ser considerada confiável por possuir um certificado assinado por uma entidade certificadora reconhecida. Contudo, mesmo esta entidade válida pode ser corrompida e começar a agir de maneira maliciosa produzindo conteúdos falsos ou de baixa qualidade.

Uma forma de construir esta percepção de confiança dinamicamente é assumir o uso de mecanismos de reputação. A abordagem utilizada é baseada no histórico de ações das entidades provedoras de serviços e do desempenho destes. Cada ação realizada influencia diretamente na construção da própria reputação. Sendo assim, a reputação, que está atrelada a identidade única de uma dada entidade, pode ser considerada como um critério importante na confiança desta. Ademais, a reputação também pode ser vista como uma moeda de troca no fornecimento de serviços e/ou medida de qualidade ou classificação do provedor de serviços.

Assim como o DID, a reputação deve ser uma informação publicamente acessível e verificável. Desta forma qualquer possível consumidor de serviços pode avaliar a priori qual o melhor provedor antes de necessariamente requisitar algo. Com a adoção do DID, esse desafio é solucionado dado seus atributos de descentralização, tendo em vista que as ferramentas criptográficas necessárias para validar as próprias informações estão contidas em uma infraestrutura pública. ToID utiliza desta visão para implementar a reputação. Como representado na Figura 1, é apresentado o funcionamento geral da proposta, em que a entidade, identificada por um único DID, pertence a múltiplas pools. Apesar de usar o mesmo DID em pools diferentes, a reputação não será a mesma. Isto ocorre pois há contextualidade no cálculo da reputação, sendo que em cada pool a entidade pode ofertar serviços distintos e para cada pool os fatores considerados para a reputação tendem a ser variados. Uma blockchain denominada Verifiable Data Registry (VDR) mantém a informação desta reputação de forma contextual por meio de diferentes contratos inteligentes que implementam a lógica desejada por cada pool.

A VDR provê ainda um repositório de identidades e credenciais verificáveis no contexto de IDD, sendo a base da solução de confiança decentralizada proposta. Detalhes de implementação da proposta são explorados na Seção 4.

3.2. Cálculo e gestão da reputação

A reputação pode ser compreendida como altamente contextual [Botsman 2017], ou seja, a percepção de maior ou menor reputação para uma entidade depende do contexto em que aquela entidade é avaliada. Desta forma, em cenários de fornecimento de serviços, a

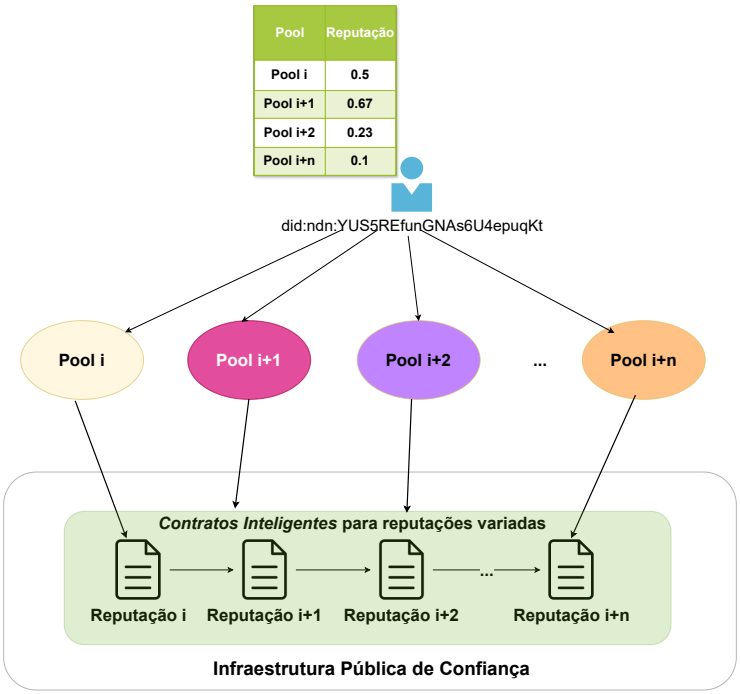


Figura 1. Arquitetura conceitual da ToID.

reputação pode considerar diversos fatores, como, por exemplo: tempo de conclusão da tarefa, complexidade da tarefa, corretude na realização de tarefas, e reputação prévia do provedor.

Neste trabalho, consideramos como fatores o tempo de conclusão da tarefa e a reputação prévia do provedor, que engloba o número de tarefas já realizadas por ele (endossos) e a reputação em si. Os endossos são critérios importantes na criação de confiança em uma *Web of Trust*, pois são tomados como provas de capacidade e comprometimento por possíveis consumidores.

A Equação 1 demonstra como é calculada a reputação na ToID. O valor $R(\lambda_t)$ é a reputação final no tempo t que será dada por uma ponderada (pelos pesos de ω_1 a ω_3) dos fatores: tempo de conclusão (α), número de endossos (β) e a reputação prévia (λ_{t-1}).

$$R(\lambda_t) = \frac{(\omega_1 \times (\frac{\alpha_{max}}{\alpha})) + (\omega_2 \times \frac{\beta}{\beta_{max}}) + (\omega_3 \times \lambda_{t-1})}{\omega_1 + \omega_2 + \omega_3} \quad (1)$$

Este é o nosso mecanismo de reputação inicialmente proposto, mas ToID é agnóstico quanto ao cálculo da reputação podendo-se utilizar diferentes abordagens existentes na literatura.

Os pesos (ω_i) refletem a importância de cada fator. Para a presente equação, utilizamos: $\omega_1 \geq \omega_2 > \omega_3$. Em suma, ToID observa a performance e endossos para incentivar os nós a manterem um padrão de qualidade na execução dos serviços mesmo que estes já possuam uma reputação anterior alta. O fator do tempo de execução reflete em maior reputação para menor tempo de execução observado (conhecido um limite máximo α_{max}). O fator número de endossos reflete em maior reputação para um maior número

de endossos (assumido um limiar máximo de endossos β_{max}). Por fim, podemos assumir que a atualização da reputação utiliza a reputação anterior com um fator de esquecimento e assim podemos assumir que:

$$\frac{\omega_1 + \omega_2}{\omega_1 + \omega_2 + \omega_3} = 1 - \frac{\omega_3}{\omega_1 + \omega_2 + \omega_3} \tag{2}$$

Para nós recém-admitidos na rede, é concedido o benefício da dúvida em relação à sua integridade. Assumimos como reputação inicial que o nó tem uma probabilidade inicial de 50% de agir corretamente em seu primeiro serviço. Essa abordagem visa a minimizar possíveis injustiças, adotando uma postura otimista em relação ao comportamento do nó. Uma visão pessimista, que presume um comportamento inadequado, pode levar à impossibilidade de prestação de serviços por ele.

Vale destacar que o consumidor também tem sua reputação afetada pelo seu comportamento. A cada serviço consumido, a reputação é atualizada sem automaticamente usando a Equação 3, na qual o consumidor recebe uma recompensa com base no tempo de resposta na confirmação de eventos (γ) vezes o incentivo ω_{inc}. Assim como o provedor de serviços, a recompensa final será impactada se o tempo for muito alto.

$$R(\lambda_t) = \lambda_{t-1} + (\frac{\gamma_{max}}{\gamma}) \times \omega_{inc} \tag{3}$$

A Figura 2 ilustra em um passo a passo do funcionamento da ToID. Na etapa *1*, o consumidor Bob realiza uma requisição de serviço para Alice, que aceita a tarefa e instancia uma contrato de serviço (SC) destinado a Bob (2). Bob então assina o contrato (3) e notifica Alice que inicia prontamente o processamento da tarefa (4). Ao terminar a execução, Alice envia o resultado para Bob (5), que confirma o recebimento ao encerrar o contrato de serviço. Por fim, a reputação é calculada automaticamente após o fechamento do contrato de serviço, sendo atualizada por meio de uma transação (6). A utilização de *smart-contract* para gestão da reputação permite uma maior de segurança no sistema, pois apenas através do contrato de serviço é possível aumentar a reputação. Ainda, é possível configurar parâmetros que inibem ataques de conluio, como, por exemplo, a definição de limiares de tempo mínimo/máximo de execução de tarefas e número máximos de serviços providos para uma mesmo consumidor.

3.3. Infraestrutura pública descentralizada de confiança

ToID tem como objetivo criar um ambiente de confiança baseado em reputação para o fornecimento de serviços. Assim, é preciso dispor de um sistema resiliente, imutável ao mesmo tempo em que permita flexibilidade na criação de aplicações e implantação de lógica de negócios nesse cenário. Com base nisso, foi proposto o conceito de uma infraestrutura pública de confiança descentralizada (do inglês, *public trust infrastructure* – PTI), apresentada no formato de um sistema distribuído de armazenamento de informações e controle de reputação. A PTI agrega a função de VDR, o livro-razão distribuído já apresentado, mas também pode viabilizar a adição de novos serviços, como ampliar as atributos dos DIDs, interoperabilidade, criação de negócios em cima de identidade e autenticação remota.

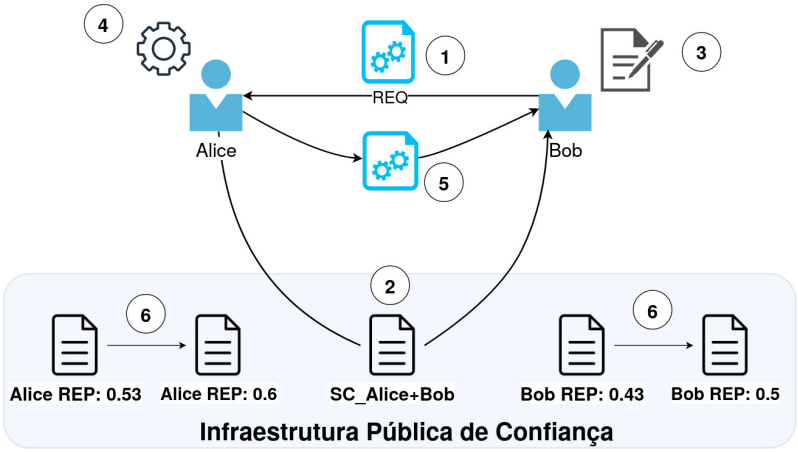


Figura 2. Tomada de decisão baseada na reputação e migração de *pools*.

A implementação desta infraestrutura foi realizada por meio de contratos inteligentes implantados em uma rede blockchain. Ao utilizar uma blockchain como plataforma, é garantido os requisitos mínimos que a proposta necessita, que visam manter a integridade da reputação assim como mantê-la globalmente acessível. ToID utiliza blockchain como uma plataforma subjacente para a implementação da PTI, sem nenhum ajuste nos blocos da própria blockchain, como, por exemplo, no algoritmo de consenso utilizado.

A PTI não necessariamente deve ser implementada por meio de uma rede blockchain. Outras tecnologias podem possibilitar uma infraestrutura distribuída para prover dados e funções (por meio de contratos inteligentes) que permita manter o esquema de reputação associado a um identificador único, independente de como a reputação seja calculada.

4. Implementação da ToID

A implementação da ToID foi realizada considerando a realização da prova de conceito de modo que fosse possível avaliar os benefícios do serviço de confiança desenvolvido. A aplicação distribuída utilizada foi desenvolvida através das redes de dados nomeados (NDN), uma vez que a mesma faz uso de infraestrutura de chave pública e que possuem aplicações que oferecem funções nomeadas de rede que podem se beneficiar de um serviço de reputação.

A ToID foi implementada em duas camada. Na camada inferior, residem os agentes aca-py (*Aries Cloud Agent* em Python [Aries 2023]), que desempenham um papel crucial na construção de aplicações de IDD. Esses agentes são responsáveis pela gestão das credenciais e conexões estabelecidas por uma entidade. Todas as credenciais são armazenadas de forma segura nas chamadas carteiras digitais. A comunicação entre os agentes é realizada utilizando o padrão de mensagens IDD: DIDComm [Hardman 2019], um protocolo de transporte agnóstico que pode ser executado sobre o protocolo HTTP, *websockets* e *Bluetooth*. Já na camada superior, está localizado a PTI que é o repositório de material criptográfico para validação de credenciais e identidades implementados através de contratos inteligentes. Nesta camada, os agentes interagem entre si utilizando DIDComm sobre NDN enquanto utilizam HTTP ou HTTPs para acessar a PTI. Isso ocorre pois a Hyperledger Besu, tecnologia de livro-razão adotada, ainda não possui suporte para NDN.

No entanto, para trabalhos futuros serão estudados sistemas de livro-razão nativos de NDN (e.g. [Zhang et al. 2019] e [Yu et al. 2023]).

Para a implementação da PTI foi utilizada blockchain permissionada, por meio da iniciativa Hyperledger [Dhillon et al. 2017]. Trata-se de um projeto de código-aberto para implementação de redes blockchain, com diferentes *frameworks* e módulos. Para a ToID, foram utilizados contratos inteligentes escritos na linguagem Solidity [Dannen and Dannen 2017] e implantados em um ecossistema baseados na EVM (*Ethereum Virtual Machine*). Esta abordagem de implementação permite a execução em múltiplas tecnologias de redes blokchain existentes sem problemas de compatibilidade. Para este trabalho, foi escolhido o Hyperledger Besu [Foundation 2024].

A adoção de contratos inteligentes permite uma maior flexibilidade na implementação das aplicações descentralizadas (do inglês, *decentralized applications* – DApps) no geral. Portanto, na ToID foi mimetizado o comportamento padrão da Hyperledger Indy através dos contratos implantados na PTI. Foram criados quatro contratos principais codependentes:

- IndyDidRegistry.sol, responsável pela criação e gestão de DIDs;
- SchemaRegistry.sol, permite a criação e gerenciamento de schemas necessários para criação de credenciais (depende do IndyDidRegistry);
- CredentialDefinitionRegistry.sol, utilizado para criação de templates para as credenciais mantendo as chaves que serão utilizadas em provas de posse (dependem do SchemaRegistry.sol); e
- ServiceRegistry.sol, contrato responsável pelo armazenamento e manutenção das reputações de cada nó (depende do IndyDidRegistry).

A Figura 3 apresenta o diagrama de sequência que descreve uma cena de uso da ToID. A entidade *Smart-Contracts* é uma abstração para todos os contratos criados. A primeira etapa envolve o ingresso dos nós na rede, assumido por um serviço de registro (o qual pode ser implementado por meio de um smart-contract).

Tanto os provedores quanto os consumidores devem ser registrados, visto que desempenham papéis transitórios. Após o registro e a inicialização da reputação, os nós estão prontos para oferecer serviços. Para consumir, o cliente emite um pacote de interesse especial em busca de um fornecedor. Após encontrar um, ambos realizam a consulta da reputação um do outro e autenticam-se mutuamente nessa etapa. O consumidor então decide se conecta com o provedor para requisitar o serviço desejado. O provedor cria um contrato de serviço e solicita sua assinatura. Se assinado, a tarefa é enviada pelo cliente, processada e, por fim, o resultado é enviado ao consumidor. A última etapa envolve o término do contrato, no qual o cliente deve assinar o contrato através de uma função específica. Essa etapa é crucial para o cálculo das reputações tanto do consumidor quanto do produtor.

5. Prova de Conceito

Avaliação do funcionamento e benefício da ToID se baseou no uso de uma aplicação distribuída sobre a arquitetura de Redes de Dados Nomeados (do inglês, *Named-Data Networking* — NDN) [Zhang et al. 2014]. A NDN é uma arquitetura distribuída, que oferece funções de redes nomeadas e segurança intrínseca, baseada no uso de infraestrutura de chave pública (do inglês, *Public Key Infrastructure* – PKI). Assim, para que

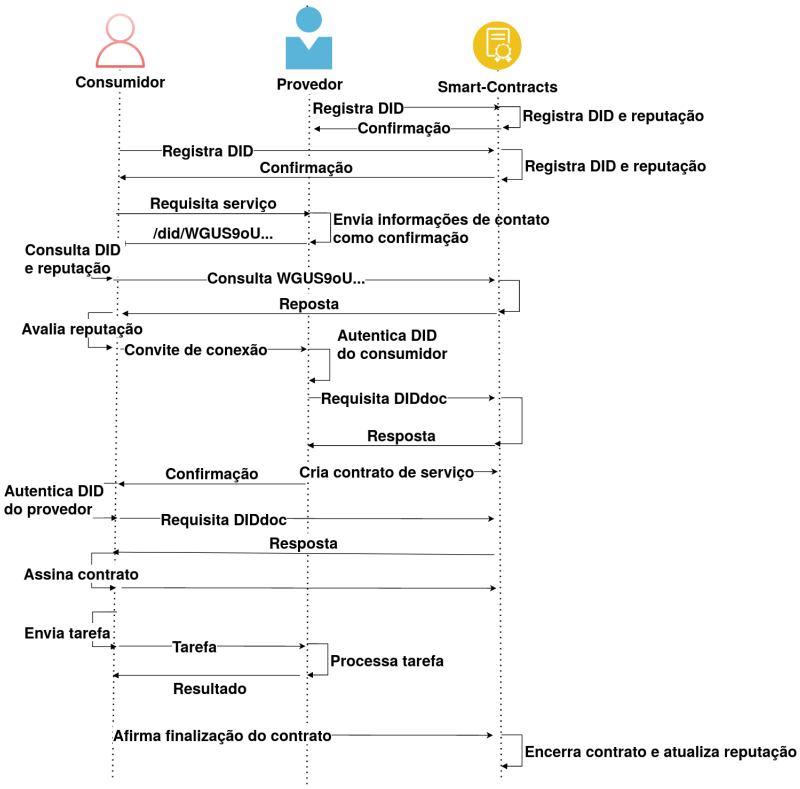


Figura 3. Funcionamento geral da implementação da ToID.

uma entidade ofereça serviço na NDN, é necessário a realização prévia de um processo de autenticação mútua entre os nós comunicantes para garantir a transmissão das âncoras de confiança e a cadeia de certificação seja iniciada. Em geral, esse processo é realizado através de um canal *out-of-band* e apenas certifica a autenticidade dos nós envolvidos na comunicação.

A NDN adota o modelo *pull-based* para requisição de conteúdo. Ou seja, um consumidor deve enviar um pacote de Interesse contendo o nome do conteúdo que deseja obter (e.g. */ufba/ic/redes/aula2.pdf*). O detentor do conteúdo, por sua vez, responde à requisição enviando um pacote de Dados pelo caminho reverso. Tal estratégia funciona bem para conteúdos estáticos (e.g., páginas web ou arquivos no geral). Contudo, quando se trata de aplicações que fazem uso de conteúdos gerados sob demanda, a partir de funções nomeadas fornecidas por múltiplos provedores de serviços, a reputação pode ser um fator considerado na escolha do serviço procurado, uma vez que nós podem estar sujeitos a falhas e/ou comportamentos diferentes.

O exemplo do cenário de computação na borda em NDN, retratado na Figura 4, ilustra o problema. O consumidor C deseja realizar o processamento remoto de um conjunto de dados de sensoriamento. O nó C, então, busca provedores desse serviço ao enviar um pacote de interesse especial de requisição (REQ), contendo o DID do consumidor (`nodeID`) e tipo de serviço (*service-type*): `/ndn/home/REQ/<nodeID>/service/<service-type>`. Em funções nomeadas podem haver diversos tipos de serviços, como processamento, armazenamento, encaminhamento, dentre outros. Ademais, cada serviço pode ter uma forma diferente de

calcular a reputação, de acordo com o contexto associado a este.

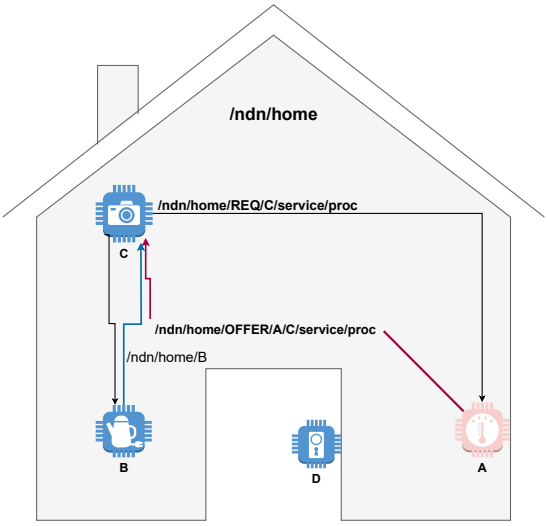


Figura 4. Funções nomeadas em cenário de provedores sujeitos à falhas.

Ao receber a requisição, os dispositivos A e B respondem oferecendo seus serviços emitindo um novo pacote especial de interesse de oferta (i.e. `/ndn/home/OFFER/<providerDID>/<consumerDID>/service/<service-type>`), que contém o DID do provedor (i.e. Alice), o DID do consumidor extraído da REQ (i.e. Bob), além do tipo do serviço que pode ser um identificador numérico para cada tipo. Nesse caso, o identificador do serviço **1** está associado a um serviço de processamento de dados. A estratégia de encaminhamento multicast foi adaptada para lidar com a lógica de mensagens da ToID (i.e. ToID-multicast). Para esse fim, os pacotes de REQ são intencionalmente inundados na rede até k saltos, sendo k um parâmetro de configuração.

No exemplo aqui discutido, contudo, há o risco de que C selecione inadvertidamente A como seu provedor de serviços, presumindo que ele é confiável devido ao seu certificado válido. Nesse cenário, A poderia explorar essa confiança para realizar ataques e atrasar ainda mais o processamento de C, potencialmente levando a um processamento inválido das tarefas que pode se prolongar indefinidamente. Para mitigar esse risco, a ToID foi adaptada para integrar-se ao contexto das NDN utilizando o esquema de nomeação citado, como representado na Figura 5.

A integração de Identidade Digital Descentralizada (IDD) com a arquitetura NDN proporciona benefícios mútuos para ambas as tecnologias. No caso da IDD, a NDN oferece maior escalabilidade, pois não depende de endereços IP para comunicação entre agentes e utiliza um canal nativamente seguro, com cada pacote de dados criptografado. Por outro lado, a NDN se beneficia da IDD ao obter uma identidade globalmente única, com uma reputação associada a ela.

Na Figura 5, é ilustrada essa integração. Cada entidade possui um Identificador Descentralizado (DID) que, na NDN, é convertido em um nome utilizado no processo de roteamento. No primeiro passo, Bob emite um interesse especial de requisição de serviço no formato NDN: `/ndn/home/REQ/<nodeDID>/service/<service-type>`. Esse pacote é propagado na rede por meio de inundação até alcançar um provedor, que res-

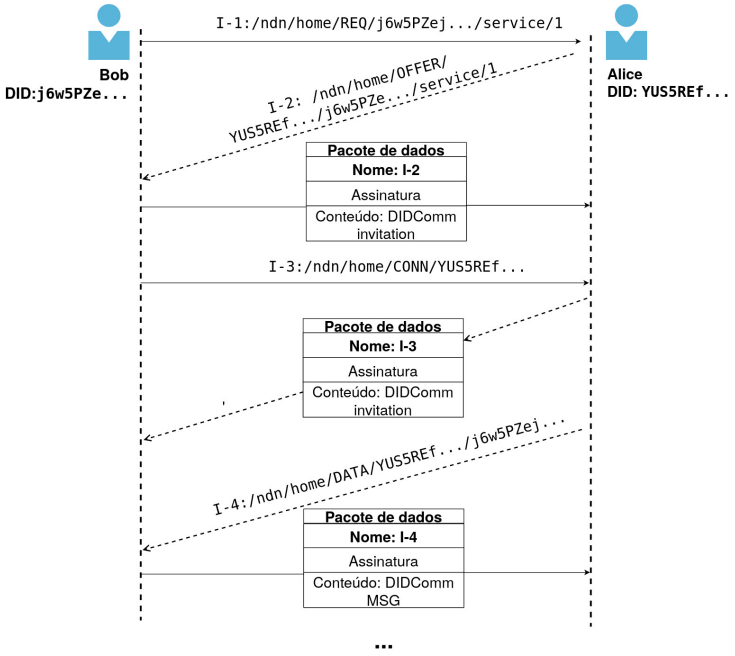


Figura 5. Funcionamento de IDD sobre NDN na ToID.

ponde com outro interesse especial de oferta: `/ndn/home/OFFER/<providerDID>/<consumerDID>/service/<service-type>`. Os nós utilizam os nomes presentes nos interesses para retornar os dados necessários para a conexão.

Bob solicita a conexão usando um pacote de dados que contém um convite no padrão DIDComm. Alice, ao receber o convite, decide aceitá-lo e avisa Bob através de um novo pacote de dados. Com a conexão estabelecida, Alice pede que Bob envie a tarefa para execução. A tarefa é enviada usando uma mensagem DIDComm dentro de um pacote de dados criptografado NDN. Essa abordagem foi baseada no trabalho de [Król et al. 2018].

Na cenário de avaliação da ToID através da NDN, os provedores também podem proativamente divulgar os serviços ofertados emitindo *beacons* periódicos usando o nome: `/ndn/home/SERVICOS/<providerDID>/<service-list>`, em que *service-list* traz todos os serviços do nó no formato de uma lista de identificadores. Essas informações são captadas pela estratégia de encaminhamento para armazenamento em *cache* e em seguida são repassadas até alcançar o número máximo de saltos.

5.1. Modelo de falhas e ameaças

Para o modelo de falhas, foi assumido que os canais de comunicação possuem caracterısticas fair lossy. Ou seja, não criam ou duplicam mensagens, e podem perder as mesmas, embora mensagens são entregues a termo por meio de um mecanismo robusto de retransmissão em caso de eventuais perdas de mensagens. A rede subjacente garante a criptografia das mensagens que não podem ser adulteradas no canal de comunicação. Além disso, os nós podem falhar por colapso ou executar ações arbitrários que desviam do algoritmo especificado, de forma maliciosa ou não intencional, por exemplo a partir de um bug ou uma condição intermitente.

Dentre os comportamentos maliciosos, o modelo de ameaças considera:

1. nós desonestos: entidades entram na rede apenas para realizarem ataques diretos aos clientes (e.g. DoS) ou inundar a rede com falsas requisições;
2. personalidade dinâmicas: nós tendem a agir de maneira imprevisível alternando entre um bom e mau comportamento; e
3. ataques *churn*: nesse cenário de ataque, o nó, que sofreu penalidades na reputação por ter realizado ataques contra a rede, troca sua identidade e entra na rede novamente visando limpar seu histórico e realizar novos ataques.

A ToID percebe um desvio de comportamento do nó como um ataque em potencial, ainda que sem intenção maliciosa. Punições a reputação são aplicadas se acaso o provedor/cliente não obedecer os limites de tempo de resposta, ou for avaliado negativamente pelo seu comportamento, tanto no fornecimento do serviço quanto no fechamento do contrato por parte do cliente.

Uma estratégia de percepção da resposta para avaliação é, na presença de três ou mais provedores habilitados para o serviço utilizar a clássica abordagem de uma redundância modular N-upla, normalmente se utilizando redundância modular tripla [Lyons and Vanderkulk 1962] (TMR, do inglês *triple modular redundancy*). TMR mascara falha em um componente, triplicando o mesmo (no caso pela presença de três provedores do mesmo serviço) e votando entre as saídas para determinação do resultado (média ou um valor votado por maioria). Assumindo que nós maliciosos informam deliberadamente respostas divergentes dos nós honestos, é possível detectar a anomalia, e o cliente não irá finalizar o contrato como concluído com sucesso, mas sim reportar a falha apresentando provas no seu endosso de reputação. Assumimos a premissa de que uma maioria de provedores associados a um mesmo serviço sempre apresentam comportamento correto.

Para evitar ataques de *churn*, a reputação inicial do nó é definida com base na reputação média da rede, reduzindo o potencial do ataque.

5.2. Experimentos

Como uma primeira avaliação do mecanismo de reputação foi realizada uma prova de conceito que exercitou diferentes cenários de uso. A infraestrutura subjacente de rede foi emulada utilizando contêineres docker. Os experimentos consistiram em dois papéis, cliente e provedor de serviços, que possuíam agentes aca-py embutidos com o *plugin* desenvolvido para comunicação sobre NDN, que se utiliza da biblioteca python-ndn. O comportamento dos atores foi pré-determinado por meio de um *dataset* sintético representado por uma fila de eventos (i.e. requisições de serviços e tempo de processamento), definidos através de uma distribuição de Poisson. O protocolo de consenso utilizado na rede Hyperledger Besu é o QBFT [Moniz 2020]. A Tabela 1 apresenta os parâmetros utilizados e a versão das bibliotecas e sistema operacional.

Os cenários exercitados são apresentados na Figura 6. Na Figura 6(a) observamos uma execução honesta do provedor de serviços, mantendo a reputação em uma faixa ao longo da execução (entre 30% e 80%). O cenário oposto é apresentado na Figura 6(b): um atraso demasiado no tempo de resposta impacta significativamente em sua reputação, mantendo-a abaixo dos 20%, tais nós podem estar com desempenho prejudicado por problemas estruturais ou deliberadamente atrasando o resultado da computação. A Figura

Tabela 1. Parâmetros do experimento

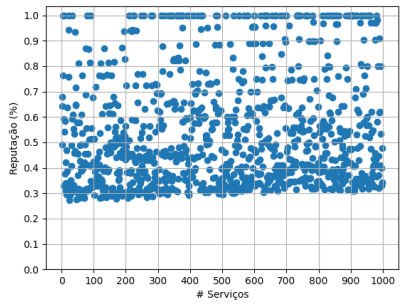
Parâmetro	**Valor**
Sistema operacional	Ubuntu 18.04 com containers Docker
versão aca-py	0.10.1
versão ndn-cxx	0.8.1
versão nfd	22.12
versão python-ndn	0.4.1
Estratégia de encaminhamento	*ToID-Multicast*
Política de *cache* da NDN	sem *cache*
DLT	Hyperledger Besu
protocolo de consenso	QBFT
$\omega_1, \omega_2, \omega_3$	4, 4, 2
$\alpha_{max}, \beta_{max}$	3600 segundos, 1000 serviços
limiar de resposta α_{max}	5min
β_{max}	1000 serviços

6(c) apresenta a dinâmica de falha do nó: o comportamento até dado instante é correto e em uma dada janela de instabilidade apresenta atrasos elevados, causando uma queda brusca em sua reputação. Por último, na Figura 6(d) é retratado a execução do modelo em um nó que apresenta oscilações no tempo de resposta entre suas execuções, devido a um ataques DoS. O modelo proposto entende que o nó pode estar passando por dificuldades e por isso o pune como forma de evitar que consumidores sejam prejudicados. Dessa forma, a reputação ficará entre 10% a 30%.

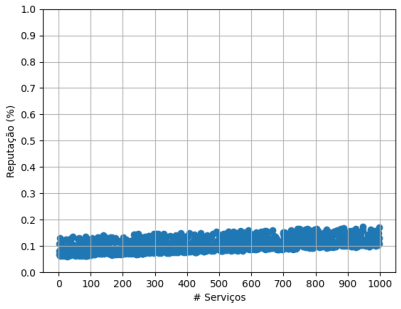
Foi avaliado também o cenário no qual o consumidor envia a tarefa para $n = 3$ provedores, de modo que possa obter um resultado fiável na presença de nós maliciosos, utilizando a abordagem TMR descrita no modelo de falhas. Na Figura 7 estão descritos os resultados desse experimento, onde na Figura 7(a) estão as reputações do provedor malicioso, configurado para atuar de forma maliciosa aleatoriamente (i.e. 50%). Já nas Figuras 7(b) e 7(c) estão os provedores autênticos que responderam corretamente à realização da tarefa. A reputação média do provedor malicioso se mantém em 20%-30% enquanto as dos demais provedores permanecem acima de 30% durante todo o período, além de possuírem reputações semelhantes tendo em vista que atenderam às mesmas requisições em um intervalo aproximado de tempo.

6. Conclusão e Trabalhos Futuros

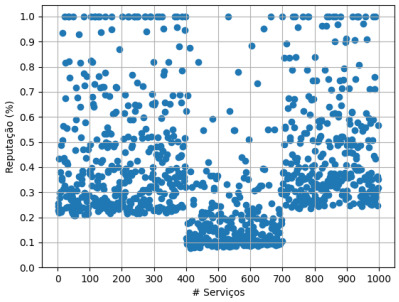
A reputação é uma medida de confiança, podendo ser obtida de diferentes formas. Na ToID, foi calculada a reputação com base nas métricas quantitativas: tempo de resposta e quantidade de endossos recebidos pelos provedores. Todavia, ao fazer isso, pode-se desassociar a reputação do provedor e direcioná-la para os serviços. Ou seja, o provedor pode possuir múltiplas reputações (uma para cada serviço oferecido), com sua reputação global sendo uma média de todas essas. Essa seria uma reputação baseada em serviços, mas podem haver outros tipos como: comportamento (e.g. bom ou mau) e participação na rede (e.g., proatividade no encaminhamento de mensagens). Ainda, destacamos o ataque de conluio. Em face de conluio, uma possibilidade é estabelecer limites no números de



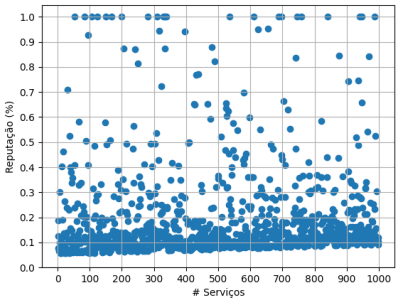
(a) Nó agindo de forma honesta.



(b) Nó deliberadamente atrasando o resultado da computação.



(c) Nó apresentando janela de instabilidade.



(d) Nó enfrentando DoS.

Figura 6. Avaliação do modelo de reputação em cenários diversos.

serviços fornecidos para um mesmo cliente (ou de possibilidades de endosso na reputação emitidas por este cliente), assim como aumentar gradativamente a recompensa pelo bom comportamento de ambos os lados. Como trabalhos futuros, investigaremos como prover maior resiliência ao sistema no conluio e outras formas de reputação a se integrar ao ToID.

7. Agradecimentos

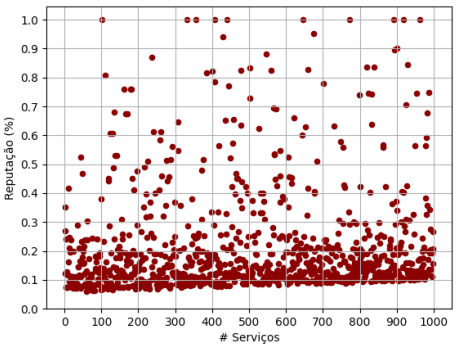
Os autores agradecem o apoio do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq), da Fundação de Amparo à Pesquisa do Estado da Bahia (FAPESB) e *Air Force Office of Scientific Research* (*award number* FA9550-23-1-0631).

Referências

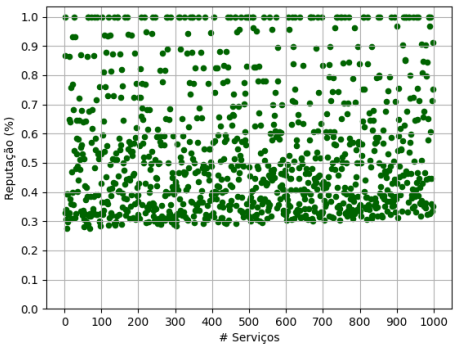
[Almasoud et al. 2020] Almasoud, A. S., Hussain, F. K., and Hussain, O. K. (2020). Smart contracts for blockchain-based reputation systems: A systematic literature review. *Journal of Network and Computer Applications*, 170:102814.

[Aries 2023] Aries, H. (2023). Hyperledger aries cloud agent python. *Accessed: Apr*, 28:2023.

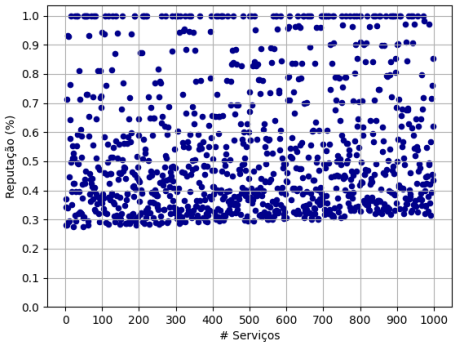
[Avellaneda et al. 2019] Avellaneda, O., Bachmann, A., Barbir, A., Brenan, J., Dingle, P., Duffy, K. H., Maler, E., Reed, D., and Sporny, M. (2019). Decentralized identity: Where did it come from and where is it going? *IEEE Communications Standards Magazine*, 3(4):10–13.



(a) Provedor Malicioso.



(b) Provedor autêntico.



(c) Provedor autêntico.

Figura 7. Avaliação do modelo de reputação em uma abordagem TMR.

[Bellini et al. 2020] Bellini, E., Iraqi, Y., and Damiani, E. (2020). Blockchain-based distributed trust and reputation management systems: A survey. *IEEE Access*, 8:21127–21151.

[Botsman 2017] Botsman, R. (2017). *Who can you trust?: how technology brought us together–and why it could drive us apart*. Penguin UK.

[Caronni 2000] Caronni, G. (2000). Walking the web of trust. In *Proceedings IEEE 9th International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WET ICE 2000)*, pages 153–158. IEEE.

[Dannen and Dannen 2017] Dannen, C. and Dannen, C. (2017). Solidity programming. *Introducing Ethereum and Solidity: Foundations of Cryptocurrency and Blockchain Programming for Beginners*, pages 69–88.

[Dhillon et al. 2017] Dhillon, V., Metcalf, D., Hooper, M., Dhillon, V., Metcalf, D., and Hooper, M. (2017). The hyperledger project. *Blockchain enabled applications: Understand the Blockchain ecosystem and how to make it work for you*, pages 139–149.

[Feraudo et al. 2024] Feraudo, A., Romandini, N., Mazzocca, C., Montanari, R., and Bellavista, P. (2024). Diva: A did-based reputation system for secure transmission in vanets using iota. *Computer Networks*, page 110332.

[Fernandes et al. 2023] Fernandes, C. P., Montez, C., Adriano, D. D., Boukerche, A., and Wangham, M. S. (2023). A blockchain-based reputation system for trusted vanet nodes. *Ad Hoc Networks*, 140:103071.

[Foundation 2024] Foundation, H. (2024). Hyperledger besu. `https://www.hyperledger.org/projects/besu`. Accessed: 2024-06-05.

[Gupta et al. 2003] Gupta, M., Judge, P., and Ammar, M. (2003). A reputation system for peer-to-peer networks. In *Proceedings of the 13th international workshop on Network and operating systems support for digital audio and video*, pages 144–152.

[Hardman 2019] Hardman, D. (2019). Aries rfc 0005: Did communication. *Hyperledger. URL: https://github. com/hyperledger/aries-rfcs/blob/b40a77b05e11b0dcb7c94f24da5 97f1388220139/concepts/0005-didcomm/README. md (besucht am 28. 12. 2021)*.

[Hou et al. 2023] Hou, B., Xin, Y., Zhu, H., Yang, Y., and Yang, J. (2023). Vanet secure reputation evaluation & management model based on double layer blockchain. *Applied Sciences*, 13(9).

[Król et al. 2018] Król, M., Habak, K., Oran, D., Kutscher, D., and Psaras, I. (2018). Rice: Remote method invocation in icn. In *Proceedings of the 5th ACM Conference on Information-Centric Networking*, pages 1–11.

[Lyons and Vanderkulk 1962] Lyons, R. E. and Vanderkulk, W. (1962). The use of triple-modular redundancy to improve computer reliability. *IBM journal of research and development*, 6(2):200–209.

[Moniz 2020] Moniz, H. (2020). The istanbul bft consensus algorithm. *arXiv preprint arXiv:2002.03613*.

[Singh et al. 2020] Singh, R., Donegan, A., and Tewari, H. (2020). Framework for a decentralized web. In *2020 30th International Telecommunication Networks and Applications Conference (ITNAC)*, pages 1–7. IEEE.

[Tan et al. 2023] Tan, K. L., Chi, C.-H., and Lam, K.-Y. (2023). Survey on digital sovereignty and identity: from digitization to digitalization. *ACM Computing Surveys*, 56(3):1–36.

[Yu et al. 2023] Yu, T., Xie, H., Liu, S., Ma, X., Patil, V., Jia, X., and Zhang, L. (2023). Cledger: A secure distributed certificate ledger via named data. In *ICC 2023-IEEE International Conference on Communications*, pages 5091–5096. IEEE.

[Zhang et al. 2014] Zhang, L., Afanasyev, A., Burke, J., Jacobson, V., Crowley, P., Papadopoulos, C., Wang, L., Zhang, B., et al. (2014). Named data networking. *ACM SIGCOMM Computer Communication Review*, 44(3):66–73.

[Zhang et al. 2019] Zhang, Z., Vasavada, V., Ma, X., and Zhang, L. (2019). Dledger: An iot-friendly private distributed ledger system based on dag. *arXiv preprint arXiv:1902.09031*.

[Zimmermann 1992] Zimmermann, P. (1992). *PGP User's Guide*. Phil Zimmermann. Version 2.0.