Identidade descentralizada e Blockchain: Um estudo exploratório sobre as oportunidades e desafios das soluções existentes

Maurício Pinto[1], Alan Veloso[1,2], Bruno Evaristo[1,3], Jeffson C Sousa[1,3], Billy Pinheiro[4], Antônio Abelém[1]

[1] Grupo de Pesquisa em Rede de Comutadores e Comunicação Multimídia (GERCOM)
Laboratório de Tecnologias de Informação e Comunicação (LabTIC)
Universidade Federal do Pará (UFPA) – Belém – PA – Brasil

[2]Instituto de Colaboração em Blockchain (iCoLab)
Porto Alegre – RS – Brasil

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

[4]Amazônia Blockchain Solutions (Amachains)
Parque de Ciência e Tecnologia do Guamá (PCT Guamá), Espaço Empreendedor
Belém – PA – Brasil

mauricio.pinto@itec.ufpa.br, aveloso@ufpa.br, {elderb, jcsousa}@cpqd.com.br,
billy@amachains.com, abelem@ufpa.br

Resumo. *O objetivo deste estudo é fornecer um levantamento das principais soluções atualmente utilizadas em redes de plataformas DID. Os resultados obtidos através da revisão sistemática da literatura cinzenta indicam que, embora soluções consagradas como Ethereum e Hyperledger Indy sejam amplamente utilizadas, novos modelos de soluções estão surgindo, com transações mais rápidas e menor consumo de recursos computacionais.*

Abstract. *The objective of this study is to survey the main solutions currently used in networks of DID platforms. The results obtained through the systematic review of the gray literature indicate that, although established solutions such as Ethereum and Hyperledger Indy are widely used, new models of solutions are emerging, with faster transactions and lower computational costs.*

1. Introdução

A Tecnologia de Registro Distribuído (*Distributed Ledger Technology* - DLT) entrega propriedades como descentralização, imutabilidade, transparência e auditabilidade às aplicações [Monrat et al. 2019], sendo a Blockchain um tipo de DLT popularmente utilizado e tratado como sinônimo de DLT neste trabalho.

Diferentes redes Blockchain, como Sovrin Network (Hyperledger Indy) e Ethereum Mainnet (Ethereum), são utilizadas em plataformas de Identidade Descentralizada (*Decentralized Identity* - DID) [Čučko and Turkanović 2021]. Cada rede tem propriedades específicas que podem influenciar na escolha para a construção de plataformas de

DID. Este trabalho visa fornecer um levantamento da literatura cinzenta[1] com o estado da prática das principais soluções Blockchain adotadas pela indústria e empregadas nas redes utilizadas pelas plataformas de DID.

Estudos sobre DID e Blockchain [Siqueira et al. 2021, Čučko and Turkanović 2021, Schardong and Custódio 2022, Nokhbeh Zaeem et al. 2021] não abordam as plataformas usadas atualmente em produção e particularmente não avaliam as soluções utilizadas pelas redes. Sendo assim, a principal contribuição deste trabalho é cobrir o conjunto de soluções Blockchain utilizadas pelas plataformas de DID, possibilitando aos interessados um levantamento de possibilidades para a construção de redes para DID. Uma contribuição secundária é apresentar as redes existentes utilizadas pelas plataformas DID.

Para alcançar o objetivo do estudo, foi realizada uma revisão sistemática da literatura cinzenta a fim de identificar as soluções Blockchain usadas pelas plataformas de DID. Foram analisados e examinados em detalhes 110 conteúdos que mencionam plataformas de DID, com vistas a identificar as plataformas e as redes Blockchain utilizadas. As características das redes, como permissividade, ano de lançamento, país ou continente de origem e forma de precificação, foram coletadas e apresentadas na seção correspondente. As informações coletadas e características mencionadas permitem orientar o processo de seleção para adoção de uma dessas redes Blockchain na construção de uma plataforma DID, considerando fatores como a idade da rede e o país de origem.

Este trabalho está organizado da seguinte forma: a Seção 2 apresenta as soluções utilizadas pelas redes das plataformas de DID e suas características, e a Seção 3 finaliza com uma discussão dos resultados e possíveis trabalhos futuros.

2. Soluções Blockchain para Plataformas de Identidade Decentralizada

Esta seção apresenta o resultado do levantamento de soluções Blockchain usadas por plataformas de DID. Dos 110 materiais coletados, foram encontradas 61 plataformas. Destas, 34 estão ativas, três não mencionaram solução específica, quatro não permitiram definir a solução e uma usa mais de uma rede Blockchain. A Tabela 1 apresenta redes utilizadas por cada plataforma DID. A tabela inclui permissividade, lançamento, origem, algoritmo de consenso, precificação e solução-base.

2.1. Blockchains Não-Permissionadas

Uma Blockchain não-permissionada permite que qualquer pessoa (física ou jurídica) participe da rede, lendo ou gravando dados [Helliar et al. 2020]. No contexto de DID, uma rede não-permissionada pode ser usada para armazenar e gerenciar DIDs e informações relacionadas de maneira segura e descentralizada. Ao se franquear a participação na rede e a leitura ou gravação de dados na Blockchain facilita-se a criação e a gestão de DIDs.

A Blockchain mais utilizada para essa finalidade é a Ethereum, mas a rede Solana e as soluções derivadas do Bitcoin, como Litecoin e Namecoin, também são utilizadas (ver Tabela 1). Todavia, o uso de uma Blockchain não-permissionada pode ter riscos, pois qualquer participante pode fazer alterações na rede. Logo, é importante projetar o sistema DID para mitigar tais riscos e garantir a integridade e a segurança do sistema.

[1] Materiais e pesquisas produzidos por organizações fora dos canais de publicação e distribuição comerciais ou acadêmicos tradicionais, analisando vantagens, problemas e aplicabilidade de cada uma delas. Os tipos comuns de publicação de literatura cinzenta incluem relatórios (anuais, de pesquisa, técnicos, de projeto, etc.), documentos de trabalho, documentos governamentais, *white papers* e avaliações. [Paez 2017]

Rede	Uso	Permissividade	Lançamento	Origem	Consenso	Precificação	Solução
Ethereum Mainnet	12	Não-permissionado	2015	Suíça	PoS	Transação	Ethereum
IDChain	1	Não-permissionado	2016	Suíça	PoA	Transação	IDChain
Hypercore Network	1	Não-permissionado	2016	Global	-	-	Hypercore
Litecoin Testnet	1	Não-permissionado	2011	Estados Unidos	PoW	Transação	Litecoin
Namecoin	2	Não-permissionado	2011	China	PoW	Transação	Namecoin
Solana Network	1	Não-permissionado	2018	Estados Unidos	PoS	Transação	Solana
ChainZy	1	Não-permissionado	?	Reino Unido	-	-	ChainZy
Consortium Network	1	Permissionado	?	Europa	?	?	Hyperledger Fabric
EBSI	1	Permissionado	2018	Europa	IBFT	Assinatura	Hyperledger Besu
IDunion Network	1	Permissionado	2021	Europa	RBFT	?	Hyperledger Indy
Sovrin Network	6	Permissionado	2017	Estados Unidos	RBFT	Assinatura	Hyperledger Indy
Agnóstico	3	-	-	-	-	-	-
Indefinido	4	-	-	-	-	-	-

Legenda: (?) Não identificado, (-) Não se aplica.

Tabela 1. Redes Blockchain usadas em aplicações de DID.

2.1.1. Ethereum

A Ethereum[2] é a solução Blockchain mais utilizada entre as redes de plataformas de DID, com aproximadamente 45% do total. A Ethereum oferece várias características que a tornam adequada para o gerenciamento de DID, incluindo contratos inteligentes, interoperabilidade, auto-soberania, personalização e padrões para DID, como o ERC-725 e ERC-735. Essas características podem ter pesado na escolha da Ethereum por grande parte das plataformas analisadas neste estudo.

2.1.2. Litecoin

A solução Litecoin[3], uma criptomoeda baseada no Bitcoin, é utilizada apenas pela plataforma de DID UniquID. Embora possa ser usada para armazenar e gerenciar identidades, ela não foi projetada especificamente para esse fim e, por isso, não oferece a funcionalidade de contrato inteligente da Ethereum. Embora o Litecoin tenha tempos de confirmação de bloco mais rápidos que o Bitcoin, outras soluções, como a Ethereum, proveem mais funcionalidade e flexibilidade para a construção de sistemas de DID.

2.1.3. Namecoin

A solução Namecoin[4] é usada pela plataforma CertCoin e é uma solução de DNS descentralizada baseada em Blockchain que permite registrar e gerir nomes de domínio de forma descentralizada. O Namecoin usa um mecanismo de consenso descentralizado e criptografia semelhante ao Bitcoin, tornando-o seguro para armazenar informações pessoais. No entanto, o Namecoin é principalmente uma solução de DNS e pode não ter o mesmo nível de funcionalidade que o Ethereum ou outras soluções projetadas especificamente para a gestão de DID.

[2] https://ethereum.org/
[3] https://litecoin.org/
[4] https://www.namecoin.org/

2.1.4. Solana

O Civic Pass[5] é uma plataforma de DID projetada para lidar com muitas transações por segundo. Ela é baseada na rede Solana[6], uma solução de alto desempenho com um mecanismo de consenso exclusivo, escalabilidade, eficiência energética e um ecossistema de ferramentas e recursos para desenvolvedores. Embora a Solana ainda não seja amplamente adotada para a gestão de DID, sua escalabilidade e sua eficiência a tornam promissora para esse tipo de aplicação.

2.2. Blockchains Permissionadas

Uma Blockchain permissionada é um tipo de Blockchain cujo acesso à leitura ou à gravação de dados é restrito a determinados participantes [Helliar et al. 2020]. Esses podem ser emissores de DID, verificadores e outras partes confiáveis. O uso de uma Blockchain permissionada pode ajudar a garantir a integridade e a segurança do sistema DID, uma vez que somente as partes autorizadas podem alterar a Blockchain. Entre as soluções desse tipo utilizadas pelas redes de plataformas de DID, destacam-se as da Hyperledger Foundation: Besu, Fabric e Indy.

2.2.1. Hyperledger Besu

O Hyperledger Besu[7] é uma solução blockchain de código aberto compatível com a Ethereum e é utilizado pela plataforma de DID Alastria ID. Sua compatibilidade com o ecossistema Ethereum permite que ele execute contratos inteligentes e aplicativos descentralizados escritos em Solidity. Ele também assegura um elevado nível de privacidade por meio de diferentes protocolos e admite diferentes algoritmos de consenso, permitindo a criação de redes personalizadas e autorizadas para gestão descentralizada de DID.

2.2.2. Hyperledger Fabric

A solução Hyperledger Fabric[8] é uma rede Blockchain de código aberto, desenvolvida pelo projeto Hyperledger, adequada para soluções de nível empresarial, incluindo a gestão descentralizada de DID. Sua arquitetura modular permite a criação de redes personalizadas adaptáveis a casos de uso específicos. Ele admite diferentes algoritmos de consenso, como o *Practical Byzantine Fault Tolerance* (PBFT), que possibilita um processamento rápido e eficiente de transações. Por meio da criação de canais privados na rede ele protege as informações confidenciais e assegura privacidade. Por fim, suas APIs ricas e fáceis de integrar o tornam uma solução adequada para a gestão descentralizada de DID.

2.2.3. Hyperledger Indy

O Hyperledger Indy[9] é uma solução de código aberto mantida pela Hyperledger Foundation para o gerenciamento de Identidades Auto-Soberanas. Ele é utilizado pelas redes Sovrin[10] e IDunion[11] e é projetado para permitir que os indivíduos tenham controle total

[5] https://www.civic.com/
[6] https://solana.com/
[7] https://www.hyperledger.org/use/besu
[8] https://www.hyperledger.org/use/fabric
[9] https://www.hyperledger.org/use/hyperledger-indy
[10] https://sovrin.org/
[11] https://idunion.org/

sobre suas identidades, além de garantir privacidade. Com o Hyperledger Indy, é possível criar credenciais verificáveis e compartilhar seletivamente informações pessoais apenas com partes confiáveis. Ele também fornece bibliotecas e ferramentas para fácil integração com outros sistemas, tornando-o uma solução adequada para a gestão de DID.

2.3. Blockchains Alternativas

Como visto na Tabela 1, as soluções apresentadas a seguir também são classificadas como permissionadas ou não-permissionadas. Entretanto, elas são tratadas separadamente para dar destaques a novos modelos de Blockchain utilizados em plataformas de DID.

2.3.1. IDChain

O IDChain [Everest Foundation 2021] é a solução usada pela Everest na gestão de DID. Ele é uma solução descentralizada, segura e de alto desempenho que permite a criação de identidades auto-soberanas, credenciais verificáveis e recursos de privacidade. Ele é construído sobre a estrutura Substrate[12] e usa a rede Polkadot[13] para interoperabilidade com outras redes.

2.3.2. Hypercore

A plataforma de gerenciamento de DID Tradle[14] é construída sobre a rede Hypercore[15], que é uma solução descentralizada e distribuída para sistemas ponto a ponto. O Hypercore permite a criação de Hypercores, uma estrutura de dados que pode ser usada para armazenar e compartilhar identidades de forma segura e privada, com criptografia de ponta a ponta. A estrutura não-permissionada do Hypercore permite que qualquer nodo possa ingressar e participar da rede, tornando-a mais acessível. Em resumo, o Hypercore é um protocolo poderoso e flexível que permite o gerenciamento de identidade de forma segura, privada e descentralizada.

2.3.3. ChainZy

A ChainZy[16] é uma solução de gerenciamento de identidade descentralizada e acesso, usada pela plataforma de DID IDchainZ. Ela se concentra em identidade auto-soberana e usa uma rede Blockchain pública para criar credenciais verificáveis e assegurar elevado nível de privacidade. O ChainZy também possui uma estrutura permissionada e oferece bibliotecas e ferramentas para fácil integração com outros sistemas corporativos. Em resumo, o ChainZy é uma solução flexível para gerenciamento de identidade com recursos de privacidade e integração.

3. Considerações Finais

Este trabalho discute a utilização de soluções Blockchain em redes de plataformas de DID. Ele preenche uma lacuna na literatura ao incluir literatura cinzenta que é uma representação atualizada, e importante de ser considerada, do estado da prática [Paez 2017]. Além do foco estar nas soluções em vez das plataformas, fornecendo um retrato atualizado do estado da utilização de soluções em redes de plataformas de DID em produção.

[12] https://substrate.io/
[13] https://polkadot.network/
[14] https://tradle.io/
[15] https://hypercore-protocol.org/
[16] https://www.chainzy.com/

Algumas soluções utilizadas pelas plataformas de DID podem não ser adequadas para isso, mas são consideradas possivelmente por possuir características atrativas para contextos específicos. As Blockchains não-permissionadas estão sujeitas a volatilidade do mercado, em certos períodos, tornando a execução das aplicações caras e impraticáveis. A alternativa mais usual é a utilização de redes permissionadas formadas por um consórcio de organizações, cobrando uma taxa de inscrição, mesmo com os descontos para algumas organizações, ainda deixa outras de fora, como instituições de ensino e pesquisa. Nesse contexto, iniciativas voltadas para o sul global são importante para o desenvolvimento de soluções de DID nos países dessa localidade.

Agradecimentos

O presente trabalho foi realizado com apoio do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) e da Amazônia Blockchain Solutions (Amachains).

Referências

Čučko, Š. and Turkanović, M. (2021). Decentralized and self-sovereign identity: Systematic mapping study. *IEEE Access*, 9:139009–139027.

Everest Foundation (2021). Everest ecosystem: The next generation of blockchain, crypto, and identity.

Helliar, C. V., Crawford, L., Rocca, L., Teodori, C., and Veneziani, M. (2020). Permissionless and permissioned blockchain diffusion. *International Journal of Information Management*, 54:102136.

Monrat, A. A., Schelén, O., and Andersson, K. (2019). A survey of blockchain from the perspectives of applications, challenges, and opportunities. *IEEE Access*, 7:117134–117151.

Nokhbeh Zaeem, R., Chang, K. C., Huang, T.-C., Liau, D., Song, W., Tyagi, A., Khalil, M., Lamison, M., Pandey, S., and Barber, K. S. (2021). Blockchain-based self-sovereign identity: Survey, requirements, use-cases, and comparative study. In *IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology*, pages 128–135.

Paez, A. (2017). Gray literature: An important resource in systematic reviews. *Journal of Evidence-Based Medicine*, 10(3):233–240.

Schardong, F. and Custódio, R. (2022). Self-sovereign identity: A systematic review, mapping and taxonomy. *Sensors*, 22(15):5641.

Siqueira, A., Da Conceicao, A. F., and Rocha, V. (2021). Blockchains and self-sovereign identities applied to healthcare solutions: A systematic review. *arXiv preprint arXiv:2104.12298*.