Gestão de Identidades utilizando a tecnologia do Blockchain

Rodrigo Pennella Cardoso[1], Denise Goya[2]

[1]Programa de Pós-Graduação em Ciência da Computação, [2]Centro de Matemática, Computação e Cognição
Universidade Federal do ABC (UFABC)
Caixa Postal 09210-580 Av. dos Estados, 5001 - Bangú, Santo André – SP - Brazil

rodrigo.pennella@aluno.ufabc.edu.br, denise.goya@ufabc.edu.br

Abstract: O Blockchain é uma tecnologia que tem recebido grande atenção recentemente devido às suas características principais, como a descentralização, persistência, auditabilidade com alta proteção contra adulterações mesmo trabalhando com redes peer-to-peer em nós não confiáveis. Estas peculiaridades o tornam uma importante ferramenta para ser utilizada em sistemas de Gestão de Identidades. Serão apresentadas neste artigo as características que sustentam o uso do Blockchain, além da análise das estruturas existentes e suas aplicabilidades na área. Também serão discutidas as limitações que a tecnologia está sujeita atualmente.

1. Introdução

Criado em 2008, o Bitcoin é uma criptomoeda que surgiu como alternativa aos meios de pagamentos eletrônicos tradicionais, eliminando a necessidade da figura de um banco como entidade central responsável por realizar e manter os registros de todas as transações financeiras, permitindo trocas irreversíveis diretamente entre 2 pessoas [Nakamoto 2008].

O triunfo do Bitcoin se dá principalmente devido à tecnologia desenvolvida para ser seu livro-razão. Conhecida como Blockchain, essa tecnologia permite a criação de um banco de dados descentralizado, robusto e encadeado, o que proporciona a operação do Bitcoin com integridade, autenticidade e disponibilidade, ainda que seus dados estejam distribuídos em nós que não possuem confiança entre si.

O Blockchain mantém seus registros de maneira sequencial, encadeada e partilhada em todos os nós da rede peer-to-peer, de tal forma que a alteração de uma transferência já processada só possa ser feita com a alteração dos registros subsequentes no mesmo momento em mais da metade dos nós da rede [Armstrong 2016], mantendo seus registros auditáveis e não suscetíveis às alterações. Essas características permitem que o Blockchain possa ser utilizado em outros contextos.

Um sistema de gestão de identidades (GId) é uma das aplicações que pode se beneficiar das características do blockchain. Esses sistemas de GId podem ser definidos como uma plataforma que reúne as informações de identidade e acesso dos usuários. Com a utilização do blockchain essas plataformas podem ser desenvolvidas de maneira a permitir a decentralização das informações, garantindo maior confiabilidade que os sistemas tradicionais de banco de dados.

Esse artigo tem por objetivo contribuir com a ciência, através da análise das características e limitações do blockchain no que tange à sua utilização em sistemas de GId, além de analisar a possibilidade de utilização de algumas das diversas variações de blockchains existentes.

2. Blockchain

Blockchain é o nome dado para a tecnologia de uma estrutura de banco de dados encadeado, usualmente desenvolvido para trabalhar de maneira distribuída através de uma rede peer-to-peer. [Nakamoto 2008] O Blockchain é composto por diversos blocos encadeados, sendo que cada um é formado pelo agrupamento de várias transações. Cada bloco recebe em seu cabeçalho um valor Hash, uma marcação de tempo e o valor Hash do bloco anterior a ele [Narayanan et al. 2016]. A sequência de encadeamentos de cada bloco com seu antecessor cria uma cadeia voltando até o primeiro bloco já criado, que leva o nome de bloco gênese.

A rede peer-to-peer por trás da tecnologia complementa a funcionalidade do banco de dados. Com os dados disseminados por diversos computadores espalhados pelo mundo, além de garantir a disponibilidade das informações,

uma tentativa de alteração no banco de dados em um dos nós da rede, mesmo que recalculada todas as assinaturas mantendo o encadeamento, destoa dos outros nós, sendo considerada inapta, não afetando a integridade dos dados como um todo.

3. Gestão de Identidades em Blockchains

Embora tenha sido concebido para o armazenamento de transações financeiras, o Blockchain tem se mostrado eficiente em diversas outras aplicações após realizadas as devidas adaptações necessárias para sua utilização, como é o caso de projetos como o Namecoin [nam 2017] e o sistemas de Gestão de Identidades (GId) Blockstack [Ali et al. 2016].

3.1. Implementações de GId em Blockchains

Atualmente existem alguns projetos de sistemas de gestão de identidades que utilizam-se de algum Blockchain existente para manter seus registros, como é o caso do Binded [bin 2017], uma plataforma online que realiza o registro de qualquer material áudio visual no Blockchain do Bitcoin com o intuito de garantir a informação de direitos autorais de forma gratuita, segura e aberta para que qualquer pessoa possa pesquisar e auditar as informações.

Outro projeto que faz uso do Blockchain do Bitcoin é o ShoCard [sho 2017], uma startup que almeja unificar em uma única plataforma a gestão de identidade de seus usuários em todos os níveis, permitindo desde a autenticação básica em sites sem a utilização dos tradicionais métodos de usuário e senha, chegando até ao fornecimento de soluções de identificação para validar compras de cartão de crédito ou mesmo a autenticação dos passageiros de companhias aéreas através do registro da autenticação digital de passaportes no Blockchain do Bitcoin.

3.2. Limitações das implementações de Gestão de Identidades em Blockchain

Os principais problemas enfrentados nas implementações de gestão de identidades em Blockchain estão atrelados às particularidades do Blockchain no qual a solução é desenvolvida. No caso do Blockchain do Bitcoin, o qual a maior parte das soluções atuais foi desenvolvida, entre as principais limitações destacam-se principalmente o fato de que o limite de dados de cada transação é da ordem de quilobytes e o intervalo de criação de blocos é de cerca de 10 minutos [Nakamoto 2008], o que resulta em uma banda máxima de registro de informações que pode ser considerada lenta e pequena em comparação aos sistemas tradicionais, limitando o registro de grandes quantidades de informações rapidamente como ocorre em bancos de dados tradicionais.

Ademais, embora o Bitcoin seja o Blockchain com maior número de nós ativos, ainda está sujeito à concentração da mineração, e portanto, suscetível ao ataque conhecido como ”Ataque dos 51%”, onde mais da metade dos nós da rede se reúnem para violar os dados, comprometendo a segurança da aplicação.

3.3. Comaparativo entre Blockchains para sistemas GId

Entre as características elementares que impactam na utilização do Blockchain em uma solução de gestão de identidades, pode-se destacar: a taxa máxima de inserção e atualização de dados, o nível de segurança provido e o processo de mineração dos blocos que tem impacto no custo e desempenho final da solução. Podemos classificar os Blockchains existentes em 2 tipos: públicos e os privados.

A Tabela I apresenta as diferenças entre os dois tipos de Blockchains.

Tabela 1. Comparativo entre blockchains públicos e privados

	Público	Privado
Confirmação das Transações	Lento	Rápido
Segurança	Utiliza algoritmos de consenso, como Prova de Trabalho ou Prova de Participação	Aprovação prévia dos participantes
Leitura e Escrita	Públicas	Restrito a usuários com permissão

Os Blockchains públicos como é o caso do Bitcoin, são capazes de prover uma forma diferente da atual para um sistema de gestão de identidades. Sem uma entidade central e sem a necessidade de uma estrutura de servidores, são a solução ideal para sistemas seguros e distribuídos dispensando os investimentos em infraestrutura de servidores e aplicações.

Já os Blockchains privados são desenvolvidos e mantidos por uma ou mais instituições privadas, que criam sua própria rede de servidores e suas próprias regras de acordo com as necessidades de cada aplicação, mantendo as leituras e escritas com acessos restritos.

Dentre os Blockchains públicos mais utilizados atualmente destacam-se o Bitcoin, Ethereum e LiteCoin. O Bitcoin e Litecoin são as plataformas mais antigas do Blockchain e foram desenvolvidas para serem sistemas de transações bancárias. Por esse motivo, elas contam com uma capacidade pequena de armazenamento de dados, com blocos gerados a cada 10 e 2,5 minutos respectivamente.

Por outro lado, o Ethereum é uma plataforma recente e foi concebida com o intuito de ser capaz de executar contratos e aplicações decentralizadas, mantendo as características chaves do Blockchain do Bitcoin. O resultado é uma solução com maior capacidade de armazenamento de dados, com a confirmação das transações de forma mais rápida (cerca de 12 segundos, contra 10 minutos do Bitcoin) além de mitigar o problema de concentração da mineração dos blocos, que poderia trazer problemas de segurança a aplicação.

4. Conclusão

O Blockchain tem se mostrado uma excelente alternativa às tecnologias tradicionais utilizadas em gestão de identidades, impulsionada pelos ganhos em segurança, disponibilidade e até mesmo custos operacionais. Contudo uma série de desafios técnicos deve ser superada para sua utilização em larga escala em aplicações que exigem um grande fluxo de dados.

Destaca-se entre os desafios centrais: a necessidade de aumento da taxa máxima de inserção de registros, que tem se mostrado um limitante importante para sua ampla utilização, e o uso excessivo de energia no processo de mineração.

Dentre os Blockchains existentes, o Ethereum tem se mostrado a melhor opção para criação de ferramentas de Gestão de Identidades, uma vez que por se tratar de uma plataforma de Blockchain já voltada para a criação de aplicações decentralizadas, uma série de melhorias de desempenho e segurança foram concebidas em relação ao Blockchain do Bitcoin.

Referências

(2017). Binded: Copyright made simple. https://binded.com/. Data de Acesso: 4 Set. 2017.

(2017). Namecoin. https://namecoin.org/. Data de Acesso: 2 Set. 2017.

(2017). Secure enterprise identity authentication — shocard. https://shocard.com/. Data de Acesso: 4 Set. 2017.

Ali, M., Nelson, J. C., Shea, R., and Freedman, M. J. (2016). Blockstack: A global naming and storage system secured by blockchains. In *USENIX Annual Technical Conference*, pages 181–194.

Armstrong, S. (2016). Move over bitcoin, the blockchain is only just getting started.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

Narayanan, A., Bonneau, J., Felten, E., Miller, A., and Goldfeder, S. (2016). *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press.