Universidade Federal de Pernambuco
Centro de Informática

Análise de otimização do Blockchain para implementação em redes IoT

Aluno: Rafael Nunes Machado
Orientador: Paulo André da S. Gonçalves

Recife
2018

Contexto

A Internet das Coisas (do inglês, Internet of Things – IoT) é definida como uma rede que conecta uma coleção de dispositivos com identificadores únicos com a Internet [1]. Estes dispositivos apresentam características de sensores ou tomadores de decisões e possuem potencial de mutabilidade programacional. Desta forma, através do identificador único e das propriedades de sensores, é possível coletar informações sobre o dispositivo e realizar operações de alteração no seu estado a partir de qualquer lugar, em qualquer momento, por outro dispositivo.

Apesar de sua grande utilidade, a Internet das Coisas levanta problemas relacionados à segurança e privacidade de seus usuários, visto o amplo compartilhamento de informações sobre suas vidas pessoais para possibilitar a tomada de decisões. Características intrínsecas desta rede como heterogeneidade de dispositivos, ausência de centralização, grande escala e, consequentemente, grande superfície de ataque amplificam esses problemas [2].

Blockchain foi o termo empregado para um sistema de blocos encadeados criptograficamente de maneira segura. Esta tecnologia pode ser considerada a base para o funcionamento do Bitcoin e outras criptomoedas existentes atualmente. O protocolo proposto em [3] tinha como objetivo propor uma rede *peer-to-peer* de pagamentos onde não fosse necessária a validação de transações por uma entidade confiável e centralizada. As características propostas do protocolo apresentam um grande potencial de usabilidade na Internet das Coisas, visto a necessidade de comunicação entre nós descentralizados de maneira segura e a manutenção da privacidade desta comunicação. A segurança no sistema do Bitcoin pode ser relacionada principalmente à necessidade de resolução de um desafio criptográfico, chamado de Proof-of-Work, para que novos blocos de transações sejam adicionadas ao seu Blockchain. Do ponto de vista de privacidade, a identidade dos usuários que realizam transações é definida por uma chave pública mutável, o que aumenta a proteção a respeito da origem dos dados.

Entretanto, o protocolo do Bitcoin foi desenvolvido com o intuito de solucionar um problema monetário e, portanto, possui definições que tornam-se inaplicáveis no mundo da Internet das Coisas [2]. Dentre definições que podem vir a ser impraticáveis para esta rede, pode-se listar as seguintes:

- Alta necessidade de recursos computacionais para validação de transações através do modelo de *Proof-of-Work*;
- Alta latência devido aos mecanismos aplicados para evitar que usuários utilizem a mesma moeda em transações distintas;
- Problemas de escalabilidade relacionadas à quantidade de mineiros na rede e a necessidade de atingir o consenso entre os mesmos.

Apesar das dificuldades de implementação listadas acima, novas criptomoedas vêm sendo desenvolvidas com tecnologias que mitigam alguns dos problemas descritos. O protocolo Ripple, por exemplo, foi criado com o intuito de substituir a validação de transações através do modelo de *Proof-of-Work* por um novo algoritmo de consenso entre os nós verificadores distribuídos [4]. Outro exemplo, é a criptomoeda IOTA que propôs um novo sistema, aprimorado a partir do Blockchain, chamado The Tangle [5]. Este, por sua vez, apresenta uma proposta de possibilitar microtransações de moedas por dados entre dispositivos conectados na Internet das Coisas.

Objetivos

Este trabalho visa um estudo aprofundado sobre as características do Blockchain que podem apresentar benefícios a partir de sua implantação em redes de Internet das Coisas. Além disso, também serão analisadas as soluções já sugeridas e aplicadas, suas vantagens, desvantagens e vulnerabilidades a tipos de ataques contra sistemas Blockchain. Por fim, também serão sugeridas possíveis melhorias para as soluções propostas.

Cronograma

Atividade	Agosto	Setembro	Outubro	Novembro	Dezembro
Elaboração da proposta					
Levantamento bibliográfico					
Revisão da literatura					
Análise das arquiteturas propostas					
Análise de possíveis melhorias					
Escrita do documento					
Preparação para apresentação					
Entrega do documento final					

Possíveis Avaliadores

Os possíveis avaliadores para este trabalho de graduação seriam os seguintes professores:

- Kiev Gama
- Ruy de Queiroz
- Vinicius Cardoso Garcia

Referências Bibliográficas

[1] R. Minerva, A. Biru e D. Rotondi, “Torwards a definition of the Internet of Things (IoT)”, Maio 2017. Disponível em: <https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf>, Acesso em 05 de abril de 2018.

[2] A. Dorri, S. S. Kanhere e R. Jurdak, “Torwards an Optimized Blockchain for IoT” em International Conference on Internet of Things Design and Implementation (IoTDI-2017), Pittsburgh, April 2017.

[3] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, 2008. Disponível em: <https://bitcoin.org/bitcoin.pdf>, Acesso em 23 de março de 2018.

[4] D. Schwartz, N. Youngs e A. Britto, “The Ripple Protocol Consensus Algorithm”, 2014. Disponível em: <https://ripple.com/files/ripple_consensus_whitepaper.pdf>, Acesso em 25 de março de 2018.

[5] S. Popov, “The Tangle”, Outubro 2017. Disponível em: <https://iota.org/IOTA_Whitepaper.pdf>, Acesso em 26 de março de 2018.

[6] A. Dorri, S. S. Kanhere, R. Jurdak e P. Gauravaram, “Blockchain for IoT Security and Privacy: The Case Study of a Smart Home” em IEEE Percom workshop on security privacy and trust in the internet of things, 2017.

[7] R. Mahmoud, T. Yousuf, F. Aloul e I. Zualkernan, "Internet of Things (IoT) Security: Current Status, Challenges and Prospective Measures" em The 10th International Conference for Internet Technology and Secured Transactions (ICITST-2015), 2015.

Assinaturas

Recife, __ de _____ de ____

_____

Rafael Nunes Machado
(Aluno)

_____

Paulo André da S. Gonçalves
(Orientador)