UNIVERSIDADE FARIAS BRITO
GRADUAÇÃO EM GESTÃO DE TECNOLOGIA DA INFORMAÇÃO (G.T.I)

ERNESTO GURGEL VALENTE NETO

SEGURANÇA DAS CRIPTOMOEDAS:
MOEDAS VIRTUAIS

FORTALEZA – CE
2019

Ernesto Gurgel Valente Neto

SEGURANÇA DAS CRIPTOMOEDAS:
MOEDAS VIRTUAIS

Artigo apresentado sobre tema de
Segurança da Informação da
Universidade Farias Brito – FFBUni.

Agradecimento especial ao Professor
Doutor Helano Matos por ter me instruído
em todo o processo de desenvolvimento e
pelo ensino dirigido na manipulação e
avaliação da Segurança de Dados.

Fortaleza – CE

2019

CRYPTOCURRENCY SECURITY: VIRTUAL COINS

Abstract

This article presents in particular a preview of the ideology behind the emergence of economic relations, represented through Bitcoin. The evolution of this article focuses on the security analysis related to the cryptocurrency system represented by Bitcoin system transactions. Presenting a brief analysis of the security infrastructure used in transactions.

Keywords: Cryptocurrency Security, Cryptocurrency, Virtual Coins, Blockchain, Information Security, Hash Algorithm, Digital Signature, Digital Certification.

SEGURANÇA DAS CRIPTOMOEDAS: MOEDAS VIRTUAIS

Resumo

Este artigo apresenta em especial uma previa sobre a ideologia por trás do surgimento das relações econômicas, representado através do Bitcoin. A evolução desse artigo do concentra-se na análise de segurança relacionado ao sistema de criptomoedas representado pelas transações do sistema Bitcoin. Apresentando uma breve análise da infraestrutura de segurança utilizada nas transações.

Palavras-chaves: Segurança das Criptomoedas, Criptomoedas, Moedas Virtuais, Blockchain, Algoritmo Hash, Assinatura Digital, Certificação Digital.

1.0 INTRODUÇÃO

Em sua infraestrutura inicial o homem realizava trocas financeiras através de produtos em que o valor era quantificado pelo comerciante diretamente em favor de outros objetos e utensílios. A evolução da troca era alavancado pela evolução do comércio, permitindo grandes quantidades de produtos serem quantificados em valor capital agregado a moeda. Com advento da globalização e da tecnologia centenas de trocas passaram a ser realizadas pelo mundo todo gerando quantidade significativa de informação e giro de capital financeiro.

A evolução do sistema comercial com advento da tecnologia e da globalização tornava-se inevitável. O Sistema financeiro se desenvolvia em conjunto com a necessidade de gerenciar a quantidade de transações e informação gerada.

O Sistema financeiro atual indica fundamentalmente da realização de pagamentos entre duas partes interessadas, dispostas em qualquer distância do mundo globalizado ao agregarem uma terceira parte confiável em sua estrutura. Uma das partes oferta um serviço ou produto específico, chamada de parte contratada ou prestadora e a segunda parte realiza pagamentos acordados pela agregação do serviço ou produto. Ambas as partes envolvidas utilizam de uma terceira para validar e executar as transações.

Este sistema de transações fortificava complexas de instituições financeiras especializadas em realizar transações. Tal maneira mais ágil permitia a transferência de quantidades significativas de dinheiro dentro de território Nacional e fluxo entre Nações. Dentro deste contexto fraudes eletrônicas têm se tornado cada vez mais comuns e tem preocupado de maneira crescente consumidores e sistemas especializados.

“Governos são bons em cortar a cabeça de redes centralmente controladas, como o Napster, mas redes puramente P2P, como Gnutella e Tor, parecem seguir em frente inabaladas.” (NAKAMOTO, apud ULRICH, 2014, p. 42). Com o advento do desenvolvimento tecnológico o formato de conexões peer-to-peer (P2P), abre espaço para o compartilhamento na internet, permitindo a disseminação de arquivos

e a preservação do anonimato na internet. Com o surgimento do Bitcoin seguindo o modelo de conexões peer-to-peer (P2P), permite a descentralização absoluta do controle do Estado através da Rede e a frustração da soberania Estatal sobre políticas uma maneira mais direta para realizar transações financeiras.

2.0 CONCEITOS

2.1 BlockChain

Fundamentalmente falando a Tecnologia Blockchain consiste na forma de um “livro de registros contábeis” distribuídos entre computadores. O registro contábil é fundamentalmente imutável, ou seja, o livro de razão registrará transações enviadas, recebidas e quantidade realizada.

Adotando principalmente a transparência como uma das suas fundamentais formas o livro cria um índice global descentralizado onde todos os computadores participantes têm como função validar os registros e dados distribuídos e compartilhados no índice agregando crescentemente novos registros, endereços, saldos, validando e repassando transações.

2.2 Algoritmo Hash

Algoritmo ou função Hash consiste em um algoritmo que codifique qualquer grande número de dados utilizando uma tabela nominada Tabela Hash que mapeará as sequências de bits indexados na tabela gerando um código através de transformações de dados. A função resultante será um código único que permitem através de transformações a validação da integridade e consistência do armazenamento de dados com segurança servindo como prova forte de que os dados não foram adulterados e encontram-se armazenados com segurança. Devido à unicidade de suas tabelas o algoritmo ou Função Hash é considerado praticamente irreversível sem uma tabela de consulta.

2.3 Assinatura Digital

Assinatura digital é uma técnica de criptografia assimétrica elaborada através da entrada de dados de uma função matemática aplicada em um algoritmo hash. A Assinatura Digital serve como modelo elaborado para garantir a autenticidade da entidade geradora, validando assim para a entidade receptora a autenticidade da entidade geradora. A agregação do Algoritmo Hash na Assinatura Digital permite criar um registro verificador que garante a validação dos dados como uma camada de proteção adicional criptografada autenticando a informação e garantindo que o conteúdo não foi adulterado.

2.4 Certificação Digital

Segundo o Serasa Anais Eletrônicos, 2019. Disponível em: <<https://serasa.certificadodigital.com.br/ecpf/>>, acessado em 17 de setembro 2019. O certificado digital é uma identificação eletrônica para pessoas e empresas, uma carteira de identidade no mundo virtual que consiste em validar a juridicidade dos documentos eletrônicos, desburocratizar processos e economizar tempo de serviços realizados pela internet.

Essa identidade digital permite funcionar como identificador único para indivíduos conectados a rede equivalente a uma carteira de identidade anexada aos processos e transações, fato importante a se ressaltar diante da versatilidade das conexões peer-to-peer (P2P) que fogem do controle do estado, na ausência de uma instituição financeira ligada diretamente a soberania jurídica e territorial.

Segundo o Diário Oficial da União Instrução Normativa RFB 1.888/2019, 2019. Disponível em: <<http://www.in.gov.br/web/dou/-/instru%C3%87%C3%83o-normativa-n%C2%BA-1.888-de-3-de-maio-de-2019-87070039>>. Acesso em 17 de setembro 2019. No que diz respeito sobre o uso obrigatório do certificado digital para declarar o uso de criptomoedas sua função consiste, Segundo AC¹ (16 de maio 2019) a intenção da normativa é evitar que crimes de lavagem de dinheiro ocorram utilizando esse tipo de transação.

¹**Autoridade Certificadora (AC).** Disponível em: <<https://www.linkcertificacao.com.br/quem-somos/>>. Acesso 17 de Setembro de 2019. **Sobre Informações sobre Normativas.** Disponíveis em: <<https://www.linkcertificacao.com.br/declarar-criptomoedas/>>. Acesso 17 de Setembro de 2019.

3.0 CRIPTOMOEDAS.

Como citado anteriormente na introdução desse artigo as criptomoedas beneficiam-se das conexões peer-to-peer (P2P) para fluírem livremente através do ambiente virtual sem a necessidade de uma instituição terceira entre destinatário e

emissor, movimentando o “dinheiro virtual” no interior de países e exterior. Com a crescente vasão das criptomoedas no mercado financeiro cada vez mais instituições têm aceitado pagamento em bitcoins ou outras formas de criptomoedas. Desde o surgimento do bitcoin cada vez mais outras criptomoedas têm surgido no mercado, tais quais são citadas na tabela a seguir.

Moeda	Descrição
Bitcoin	O Bitcoin foi criado em 2009, modelo inicial para as criptomoedas sendo considerado por muitos a primeira, seu criador permanece uma fonte anônima ainda hoje.
Cardano	O Cardano é considerada uma moeda dinâmica, com um protocolo considerado bastante robusto, criado em 2015 por Charles Hoskinson.
Ethereum	A Ethereum é considerada a segunda moeda de mais valor entre as moedas virtuais, com um sistema se assemelha bastante ao do Bitcoin, onde as operações são registradas em forma de planilha.
Litecoin	Criada em Outubro de 2011 surgindo com uma proposta de um aspecto mais leve para utilização do processamento em hardwares mais baratos e um aspecto de fácil utilização e mineração.
Stellar	Foi criada baseando-se no sistema financeiro atual com proposta inovadora para transações mais ágeis e não utilização da mineração de criptomoedas, permitindo também a utilização de transações descentralizadas, atraindo grandes parceiros como IBM.
Monero	Criptomoeda criada em 2014 agregando fortes protocolos para garantir o anonimato durante as transações e uma forma de mineração de criptomoedas mais igualitária. Porém devido a atividades ilegais o website foi fechado pela justiça em 2017.

Quadro 1 – Criptomoedas e Descrições. (Fonte elaborada pelo autor).

Segundo Frabansile, Daniela. O mercado das criptomoedas passou por expansão e diversificação e, de acordo com a plataforma Coinmarketcap, já conta com mais de 1.800 diferentes moedas digitais. Revista Época em publicação online, 04 de Novembro de 2018.

4.0 MECANISMOS DE SEGURANÇA

Devido a forte agregação de algoritmos utilizados na criptografia moderna e ferramentas de controle e validação com elevados níveis de segurança para a

validação da autenticidade das entidades participantes nas transações e averiguação de fundos financeiros utilizados entre as entidades o surgimento das criptomoedas inverte os valores dos sistemas tradicionais centralizados onde dependemos de instituições financeiras, apresentando essa nova forma de moeda virtual através de um robusto sistema de computacional.

Segundo Ulrich, Fernando. Em síntese a segurança do sistema depende de três mecanismos principais a criptografia moderna, a rede peer-to-peer e o conjunto de incentivos contidos no protocolo. Revista InfoMoney, 18 de outubro de 2016. Ainda segundo Ulrich, Fernando. No sistema a rede não possui uma entidade central fiscalizando o sistema, sobre tudo, todos os usuários monitorariam e asseguram que o sistema funcione corretamente. A rede não é controlada por ninguém específico, mas sendo supervisionada por todos na verdade.

5.0 DISCUSSÕES E RESULTADOS

A infraestrutura do BlockChain como um registro contábil fundamentalmente imutável garante elevado grau de confiabilidade no sistema de transparência das criptomoedas. Utilizando do Algoritmo Hash e da Assinatura Digital as criptomoedas se beneficiam de um elevado modelo de autenticidade computacional que combinados garantem a criação de registros e verificadores de autenticidade de conteúdo, combinados com Certificação Digital dão a essa infraestrutura a confiabilidade entre as entidades autenticadas e validadas através de identificadores únicos a segurança dos processos e transações.

6.0 CONCLUSÃO

Em análise dos algoritmos utilizados na criptografia moderna citada anteriormente nesse artigo e agregação das ferramentas de controle e validação como algoritmos de Certificação Digital, Assinatura Digital, Hash e BlockChain provêm elevados níveis de segurança comprovados computacionalmente validando

a autenticidade das entidades participantes nas transações e fundos financeiros utilizados entre as entidades. Esses mecanismos provêm elevado grau de segurança desqualificando terceiras entidades participantes em negociações e reduzindo a força Estatal sobre políticas e transações financeiras visto que várias transações podem ser realizadas sem conhecimento do estado através de conexões peer-to-peer (P2P).

6. REFERÊNCIAS

Faé, Jemuel Paulo. A Ascensão das Criptomoedas: Consequências para o Regime Monetário Internacional. Universidade Federal de Santa Catarina. 2015-01-13.

Rodrigues, Carlos Sistema Bitcoin: Uma Análise da Segurança das Transações. Revista Brasileira de Sistemas de Informações. 2017/12/28

DANIELA FRABASILE. Bitcoin, Litecoin, Ethereum: Conheça as Principais Criptomoedas. Revista Época Negócios. 01 de Novembro de 2018. Disponível em: <<https://epocanegocios.globo.com/Tecnologia/noticia/2018/09/bitcoin-litecoin-ethereum-conheca-principais-criptomoedas.html>>. Acesso 18 de Setembro de 2019.

FERNANDO ULRICH. Entendendo os riscos e a segurança do bitcoin. 18 de Outubro de 2016. Disponível em: <<https://www.infomoney.com.br/blogs/cambio/moeda-na-era-digital/post/5647890/entendendo-os-riscos-e-a-seguranca-do-bitcoin>>. Acesso 18 de Setembro de 2019.

FERNANDO ULRICH. Entendendo Os Riscos e a Segurança do Bitcoin. 18 de Outubro de 2016. Disponível em: <<https://www.infomoney.com.br/blogs/cambio/moeda-na-era-digital/post/3263090/grande-invencao-tecnologica-bitcoin-parte>>. Acesso 18 de Setembro de 2019.

FERNANDO ULRICH. Entendendo os riscos e a segurança do bitcoin. 18 de Outubro de 2016. Disponível em: <<https://www.infomoney.com.br/blogs/cambio/moeda-na-era-digital/post/3283338/grande-invencao-tecnologica-bitcoin-parte>>. Acesso 18 de Setembro de 2019.

Autoridade Certificadora (AC). Operações com criptomoedas devem ser declaradas com certificado digital. Disponível em: <<https://www.linkcertificacao.com.br/declarar-criptomoedas/>>. Acesso 17 de Setembro de 2019.

Diário Oficial da União Instrução Normativa RFB 1.888/2019, 2019. Disponível em: <<http://www.in.gov.br/web/dou/-/instru%C3%87%C3%83o-normativa-n%C2%BA-1.888-de-3-de-maio-de-2019-87070039>>. Acesso em 17 de setembro 2019.

Serasa. Certificados Digitais Serasa Experian, sua assinatura digital com validade jurídica. Disponível em: <<https://serasa.certificadodigital.com.br/manuais/>> arquivo de download disponível em: <e-CPF, e-CNPJ e NF-e>. Adata do Acesso 17 de Setembro de 2019.

Serasa. Serasa Certificados Digitais. Disponível em: <<https://serasa.certificadodigital.com.br/ecpf/>> arquivo de download disponível em: <e-CPF, e-CNPJ e NF-e>. Adata do Acesso 18 de Setembro de 2019.