A MATEMÁTICA QUE ESTABELECE O BITCOIN

Diogo Rogério Pontes da Silva (UPE)[1]
Janaína Viana Barros (UPE)[2]

d.o.i. 10.13115/2236-1499v2n20p77

Resumo

Este artigo tem por objetivo conhecer e compreender o funcionamento da tecnologia que está por trás da criptomoeda *Bitcoin*, mostrando como são utilizadas as curvas elípticas no campo da criptografia a fim de garantir a segurança e autenticidade da moeda virtual. Uma curva elíptica é uma curva algébrica definida pela equação $y^2 = x^3 + ax + b$. Com isso veremos que o protocolo *Bitcoin* utiliza o acesso a um par de chaves pública e privada do ECDSA (*Elliptic Curve Digital Signature Algorithm*), que é o Algoritmo de Assinatura Digital de Curvas Elípticas, por meio de duas operações – a adição de pontos e a duplicação de pontos – validando as transações que são feitas pela rede *Bitcoin*, sendo esta baseada em arquitetura *peer-to-peer* que é descentralizada e facilita o compartilhamento de dados.
Palavras-chave: *Bitcoin*; Curvas Elípticas; ECDSA.

Abstract

The purpose of this article is to know and to understand the operation of the technology behind the Bitcoin cryptocurrency, showing how elliptic curves are used in the field of cryptography in order to guarantee the security and authenticity of the virtual currency. An elliptic curve is an algebraic curve defined by the equation $y^2 = x^3 + ax + b$. With this we will see that the Bitcoin protocol uses the access to a public and private key pair of the ECDSA (*Elliptic Curve Digital Signature Algorithm*), through two operations - adding of points and

[1] Graduando em Licenciatura Plena em Matemática pela Universidade de Pernambuco (UPE), *Campus* Garanhuns.
[2] Prof.ª Dra. em Ciência de Materiais (UFPE).

duplicating of points -, which is the Elliptic Curves Digital Signature Algorithm, validating the transactions that are made by the Bitcoin network, which is based on peer-to-peer that is decentralized and facilitates the sharing of data.
Keywords: Bitcoin; Elliptic Curves; ECDSA.

Introdução

As criptomoedas são um tipo de moeda virtual descentralizadas, isto é, nenhum banco ou governo detém o controle sobre elas, facilitando assim as transações destas moedas de uma pessoa para outra. Por não serem controladas por bancos ou por governos, estas moedas têm taxas menores e é possível realizar as transações de qualquer lugar que tenha acesso à internet.

Assim como cada moeda ou cédula do dinheiro que costumamos ver diariamente, que contém números de série, marcas d'água e auto relevo, as criptomoedas possuem um tipo espe-cífico de segurança, a criptografia, afim de garantir mais segurança nas transações financeiras (PAVÃO, 2017). Com as moedas virtuais pode-se comprar ou vender produtos ou serviços e isso pode ser feito por qualquer pessoa e de qualquer lugar que tenha acesso à internet, sem limite mínimo ou máximo de valor. Dentre as criptomoedas existentes, destaca-se o *Bitcoin* que aqui fará parte do nosso objeto de estudo.

> O protocolo *Bitcoin* foi originalmente anunciado em um artigo publicado em novembro de 2008, o qual definiu uma forma de criptomoeda que funciona de forma pseudônima e sem depender da confiança em qualquer usuário do sistema [Nakamoto, 2008]. Esse protocolo foi desenvolvido considerando o paradigma de uma rede *peer-to-peer* (P2P) de alcance mundial, resultando em um sistema de transações financeiras de escala global (SILVA e RODRIGUES, 2016, p.525).

Na arquitetura de rede *peer-to-peer* (par-a-par, em tradução livre) cada ponto da rede funciona tanto como cliente quanto como servidor, facilitando o compartilhamento de dados sem a necessidade de um servidor central (CARVALHO, 2004). Na figura abaixo temos

exemplos de arquiteturas de redes, ao lado esquerdo um exemplo de rede comum centralizada em servidores e ao lado direito tem-se um exemplo de rede baseada em P2P, sem servidor central.

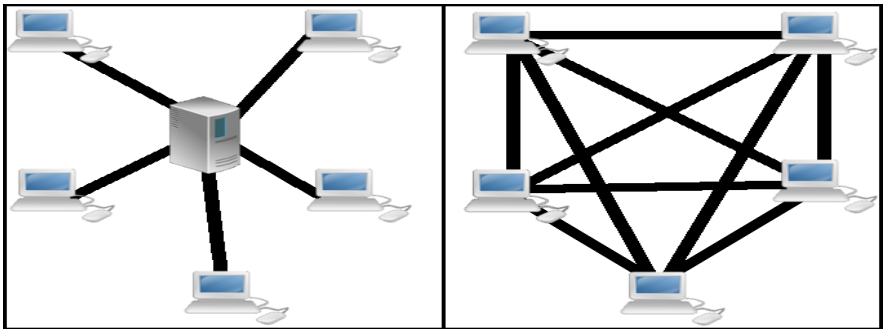

Figura 1 - Exemplos de Arquitetura de Rede. Na esquerda temos um exemplo de rede comum, centralizadas em um servidor e à direita temos um exemplo de rede baseada em P2P, sem centralização. Fonte: Autor

O objetivo deste estudo é compreender o funcionamento da tecnologia do *Bitcoin*, mostrando como esta utiliza as curvas elípticas para garantir sua segurança e autenticidade. A metodologia utilizada neste estudo foi a pesquisa bibliográfica, na qual irá propiciar a leitura, análise e compreensão de estudos relevantes ao desenvolvimento deste trabalho, ao passo que também fornecerá sustentação teórica para a sugestão de implementação da aplicação desta tecnologia no que tange aspectos de segurança e transações em contas bancárias.

A matemática do *Bitcoin*

Rykwalder (2014) declara que um dos motivos para que o *Bitcoin* pareça confuso e complicado para quem está começando a conhecê-lo é que a sua tecnologia distorce todos os conceitos de propriedade que conhecemos, uma vez que para obter bens – tradicionalmente – devemos ter as respectivas tutelas ou conceder a tutela à alguma instituição bancária. Já com o *Bitcoin* não é bem assim,

visto que a moeda não é armazenada de forma centralizada ou em instituições, por isso ninguém possui a sua tutela.

> Os próprios bitcoins não são armazenados de forma centralizada ou local e, portanto, nenhuma entidade é a sua custodiante. Eles existem como registros em um livro contábil distribuído chamado Blockchain, cujas cópias são compartilhadas por uma rede voluntária de computadores conectados. "Possuir" um bitcoin simplesmente significa ter a capacidade de transferir o controle para outra pessoa, criando um registro da transferência na Blockchain. O que concede essa habilidade? O Acesso a um par de chaves pública e privada do ECDSA (RYKWALDER, 2014).

Rykwalder (2014) explica ainda que o ECDSA (*Elliptic Curve Digital Signature Algorithm*, ou Algoritmo de Assinatura Digital de Curvas Elípticas, em português) é um algoritmo que faz uso de curvas elípticas dentro de um corpo finito para assinar os dados emitidos, de forma que os usuários possam verificar tal autenticidade enquanto que o assinante se dedica exclusivamente à concepção de novas assinaturas. Na rede *Bitcoin* os dados assinados são as transações entre os usuários. O ECDSA assina e verifica os dados em procedimentos separados, onde cada procedimento é um algoritmo formado por operações matemáticas. Enquanto o algoritmo do processo de assinatura utiliza chaves privadas, o algoritmo de processo de verificação utiliza chaves públicas.

> Uma curva elíptica é uma curva algébrica não-singular – o que significa que não possui cúspides ou auto-intersecções – definida pela equação $y^2 = x^3 + ax + b$ [...]. As técnicas de utilização de curvas elípticas na criptografia foram propostas independentemente por Miller (1985) e Koblitz (1987), servindo como uma eficiente forma de implementação de um sistema de chave pública. De acordo com seus desenvolvedores, a criptografia de curvas elípticas pode ser mais rápida e utilizar chaves mais curtas para proporcionar o mesmo nível de segurança de métodos mais tradicionais, como o RSA (MARTINS, 2018, p.16).

Uma das propriedades das curvas elípticas, por exemplo, é que uma reta não-vertical que intersecta dois pontos não tangentes na curva, intersectará um terceiro ponto desta curva. Uma segunda propriedade é que uma reta não-vertical que intersecta um ponto tangente à curva intersectará um outro ponto desta curva.

> No campo da criptografia, as curvas elípticas utilizadas são definidas sobre corpos finitos. Um corpo é um conjunto com duas operações, normalmente soma e multiplicação, que satisfazem propriedades usuais das mesmas operações com números reais. A soma deve ser comutativa, associativa, possuir elemento neutro e elemento simétrico. Já a multiplicação deve ser comutativa, associativa, distributiva, possuir elemento neutro, e todo elemento não-nulo deve possuir um inverso (MARTINS, 2018, p.16).

O protocolo *Bitcoin* faz uso de uma curva específica nomeada de secp256k1 e definida por $y^2 = x^3 + 7$ (como veremos mais adiante), conforme explica Chicarino et.al. (2017, p.13):

> No Bitcoin a chave privada é obtida gerando um número aleatório de 256bits, uma chave pública é obtida ao efetuar a multiplicação da chave privada por um ponto na curva conhecido como "ponto gerador". Ele é sempre o mesmo para todos os usuários do Bitcoin e é definido na especificação secp256k1. O resultado da multiplicação da chave privada pelo ponto gerador é um ponto na curva, este ponto é a chave pública. Os nós armazenam somente as suas chaves privadas, pois ele pode a qualquer momento gerar a pública correspondente.

Com relação à geração de chaves públicas e privadas. Martins (2018, p.25) afirma que:

> Para produzir um endereço Bitcoin, a primeira etapa a ser seguida deve ser a criação de uma chave privada *k* de 256 *bits*, que é simplesmente um número escolhido ao acaso entre 1 e 2^{256}. O método para a escolha do número é livre, mas não deve ser previsível ou repetível. Para a geração da chave pública *K*, o protocolo Bitcoin utiliza o padrão

> secp256k1, que estabelece uma curva elíptica definida sobre um campo finito de números primos. Além da curva, o padrão estabelece um ponto gerador *G*, que deve ser multiplicado pela chave privada, resultando em outro ponto na curva, que é então chamado de chave pública $K = k \cdot G$. Apesar da relação matemática entre as chaves *k* e *K*, o par somente pode ser calculado a partir da chave privada, obtendo-se então a chave pública.

A figura 2 mostra o gráfico da curva elíptica usada no *Bitcoin*.

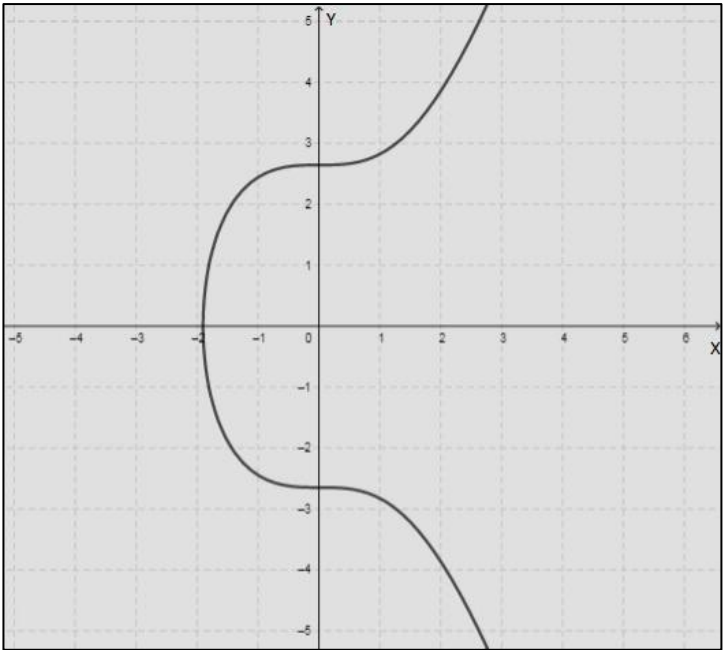

Figura 2 – Gráfico da Curva Elíptica do Bitcoin. Fonte: Autor

Deste modo, com as propriedades mencionadas anteriormente Gonzalez (2018) define duas operações:

i) Adição de ponto;

Define-se a adição de ponto **D + R = P** como reflexão do eixo X do terceiro ponto de intersecção **P** em uma reta que inclui **D** e **R**, obtendo também **P'**, como observa-se na figura 3.

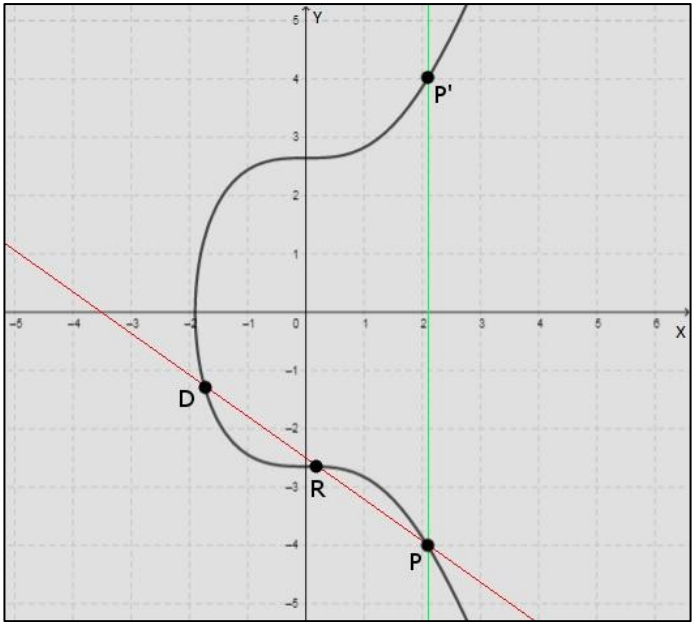

Figura 3 - Adição de ponto na curva elíptica do Bitcoin. Fonte: Autor

ii) Duplicação de ponto.

Analogamente, define-se a duplicação de pontos **D + D = P** quando encontramos a reta tangente ao ponto **D** a ser duplicado e fazemos a reflexão no eixo X do ponto de intersecção **P** e encontra-se o ponto **P'**, como mostra a figura 4.

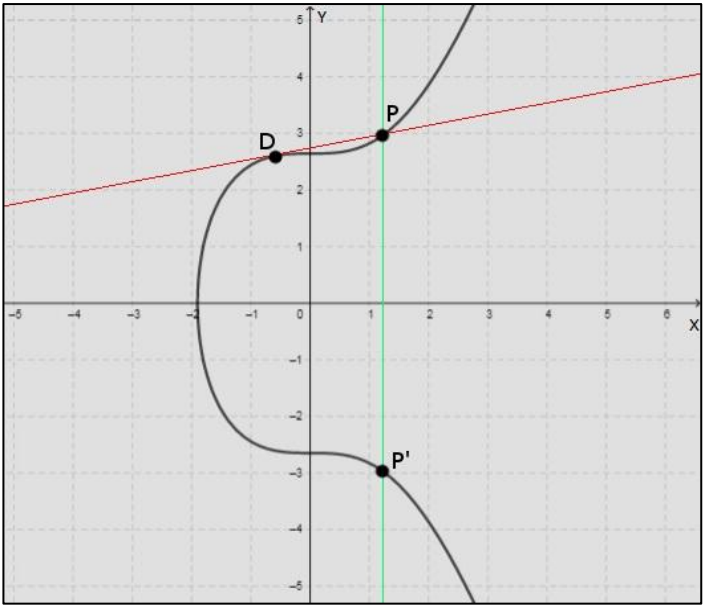

Figura 4 - Duplicação de ponto na curva elíptica do Bitcoin. Fonte: Autor

Segue que **P = a·D**, onde adiciona-se o ponto **D** a si mesmo **a** vezes, como por exemplo, **P = 5D = D + (D + (D + (D + D)))**. Desta forma, ao invés de realizar multiplicação escalar, utiliza-se uma combinação de adição de pontos e duplicações de ponto, assim, seguindo o exemplo anterior, temos:

P = 5D
P = D + (4D)
P = D + 2 · (2D)
P = D + 2 · (D + D)

Como pode-se notar, o exemplo acima foi separado em etapas de adição de pontos e duplicação de pontos. No que tange o campo do ECDSA, um corpo finito é visto como um intervalo predeterminado de números positivos que serão os resultados dos cálculos realizados. E como declara Rykwalder (2014), todos os números resultantes devem estar dentro deste intervalo, caso algum esteja fora utiliza-se o conceito do cálculo dos restos. Por exemplo, se o intervalo é de 0 a 7 e obtemos

12 como resultado, ficaremos com 1 e resto 4 e utilizamos a aritmética modular, que neste caso será indicado da seguinte forma:

$$12 \equiv 4 \, mod \, 8 \, .$$

O uso de curvas elípticas no campo do ECDSA com o conceito de corpos finitos, resulta em um gráfico semelhante ao da figura 5.

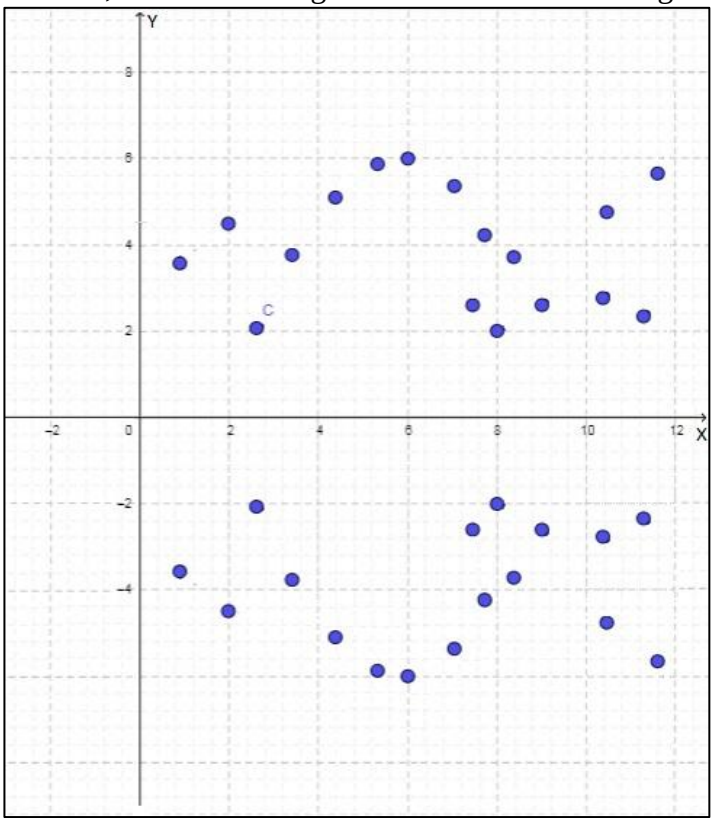

Figura 5 - Exemplo de gráfico de ECDSA com conceitos de corpos finitos. Fonte: Autor

Nota-se que a ainda existe uma simetria horizontal. E é deste modo que atua o protocolo *Bitcoin*, usando as aplicações do ECDSA com números grandes, o que resulta em um alto nível de segurança, impedindo ataques criminosos.

Portanto, conforme Brown (2010), a curva elíptica do *Bitcoin* (secp256k1) associa-se a um corpo finito $\mathbb{F}_p$ definido da seguinte forma:

$$p = FFFFFFFF\ FFFFFFFF\ FFFFFFFF\ FFFFFFFF\ FFFFFFFF\ FFFFFFFF\ FFFFFFFE\ FFFFFC2F$$
$$= 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$$

Onde a equação geral da curva $y^2 = x^3 + ax + b$ (é a partir disto que obtém-se a equação $y^2 = x^3 + 7$) sobre $\mathbb{F}_p$ será definida por:

$a =$
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
$b =$
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000007

Tendo um ponto base G, definido por:

G (Forma compactada) = 02 79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9 59F2815B 16F81798

G (Forma não compactada) = 04 79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9 59F2815B 16F81798 483ADA77 26A3C465 5DA4FBFC 0E1108A8 FD17B448 A6855419 9C47D08F FB10D4B8

E por fim, a ordem *n* de G e o seu cofator *h* são:

n = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE BAAEDCE6 AF48A03B BFD25E8C D0364141

h = 01

Esses parâmetros de *secp256k1* fazem parte de uma linhagem de soluções de curvas elípticas em corpos finitos, utilizados em criptografia e também na *Blockchain* (tecnologia que está por trás do *Bitcoin*). Assim sendo, conforme Rykwalder (2014), o algoritmo ECDSA gera uma chave privada escolhendo um número entre 1 e *n*, originando uma chave pública através de multiplicação escalar de G pelo número da chave privada, ou seja,

$$Chave\ Pública = Chave\ Privada \times G$$

Portanto, o número máximo de chaves privadas (e, consequentemente, de endereços de *Bitcoin*) é igual a *n*.

> Atualmente, a Criptografia de Curvas Elípticas - CCE - é considerada a mais eficiente, além de ser a mais utilizada

> para aplicações de blockchain. [...]. É importante ressaltar que uma chave criptográfica possui a propriedade de descriptografar a mensagem criptografada pela chave correspondente. Tanto a chave pública quanto a chave privada podem ser usadas para criptografar uma mensagem, dependendo da finalidade para a qual a criptografia é utilizada. De modo geral, a criptografia com a chave pública provê confidencialidade, enquanto a criptografia com a chave privada provê autenticidade (PIRES, 2016, p.18-19).

Embora algumas empresas não invistam em novas tecnologias, a implantação da *Blockchain* no ramo empresarial proporcionaria um maior nível de segurança, probidade, credibilidade e viabilidade na troca de informações.

> Manter o acesso de dados a uma base descentralizada, elimina a necessidade de gastos adicionais, caso haja algum problema, também possibilita o fácil acesso as suas informações sem precisar se preocupar com a burocracia ou com a demora de um órgão específico eu mantém sua informação armazenada. [...] o blockchain não abrange somente a parte financeira, as empresas podem escolher como implementá-lo, de forma que se adapte ao problema que a empresa tem, que eventualmente seria solucionado com o uso da tecnologia (LIMA, HITOMI e OLIVEIRA, 2018, P.10-11).

Por ainda adotarem sistemas tradicionais de infraestrutura e arquitetura de rede centralizada, as instituições bancárias passam por incômodos, tendentes a erros e lentidão em seus sistemas quando a rede é sobrecarregada, a partir disso se faz necessária a intervenção de especialistas – a fim de reparar as anomalias emanadas – ocasionando gastos e outros prejuízos decorrentes da perda de tempo.

> No modelo cliente-servidor o desempenho do servidor é deteriorado à medida que o número de requisições dos clientes aumenta. Em redes p2p, o desempenho geral da rede aumenta à medida que cresce o número de nós da rede. Normalmente, cada nó da rede pode realizar upload

> e download ao mesmo tempo e novos nós podem entrar na rede enquanto outros nós estão saindo, caracterizando um modelo de alta flexibilidade e ainda transparente ao usuário final (PIRES, 2016, p.24).

Antagonicamente ao que foi mencionado sobre centralização da rede das instituições bancárias, temos a *Blockchain* que é uma tecnologia segura e confiável, pois, de acordo com Pires (2016), em cada novo bloco de informações que compõe a *Blockchain* também são armazenados alguns registros do bloco anterior e, portanto, para que seja alterada alguma informação em um bloco seria necessário alterar os futuros blocos da cadeia. Destarte o uso de tal tecnologia por instituições bancárias implicara em vantagens tanto para o Banco quanto para os seus clientes.

Considerações Finais

Este artigo teve por objetivo conhecer e compreender a matemática que está por trás da tecnologia da criptomoeda *Bitcoin*. Esse estudo propôs mostrar a aplicação de curvas elípticas no âmbito da criptografia, mostrando como atua o ECDSA (Algoritmo de Assinatura Digital de Curvas Elípticas). A tecnologia que constitui o Protocolo *Bitcoin* (a *Blockchain*), que faz uso de criptografia de curvas elípticas, permite que sejam transferidos qualquer tipo de dados na rede, não apenas as criptomoedas, podendo assim ser utilizada também para outros fins.

Por meio deste trabalho foi possível estudar, do ponto de vista tecnológico, a atuação da *Blockchain* sobre a criptomoeda *Bitcoin*, buscando apresentar uma aplicação desta tecnologia para atribuição de confiabilidade e segurança entre transações bancárias.

Portanto, propõe-se que esta tecnologia seja utilizada também por instituições bancárias, autenticando as transações entre os clientes, deste modo evitaria fraudes e tornaria as transações mais rápidas e seguras, uma vez que pode-se usar os computadores dos caixas eletrônicos para constituírem a sua própria rede descentralizada

(baseada em arquitetura *peer-to-peer*) e, da mesma forma que funciona a *Blockchain*, os registros serão armazenados em cadeias de blocos de dados cujas cópias estarão distribuídas pela rede. E desta forma cada cliente teria uma chave privada *k* de 256 *bits*, onde, a partir dela, se originaria uma chave pública *K* sendo esta, associada à uma agência bancária.

Referências

Bitcoin – Open source P2P money. **Bitcoin is an innovative payment network and a new kind of money**. Disponível em <https://bitcoin.org/en/> Acesso em 30 de março de 2018.

BROWN, D.R.L. **SEC 2: Recommended Elliptic Curve Domain Parameters**. Standards for Efficient Cryptography. Certicom Research. Certicom Corp, 2010.

CARNEIRO, J.S. e ALMEIDA, K.E. **Uma Introdução às Curvas Elípticas com Aplicações para o Ensino Médio**. Universidade Estadual de Feira de Santana, BA, 2014. Ciência e Natura, Santa Maria, v. 37 Ed. Especial PROFMAT, 2015, p. 452–462. Revista do Centro de Ciências Naturais e Exatas – UFSM

CARVALHO, T.J.N. **Sistemas peer-to-peer**. Universidade de Coimbra, Departamento de Engenharia Informática – Coimbra/Portugal, 2004.

CHICARINO, V.R.L., JESUS, E.F., ALBUQUERQUE, C.V.N. e ROCHA, A.A.A. **Uso de Blockchain para Privacidade e Segurança em Internet das Coisas**. Universidade Federal Fluminense, 2017.

GONZALEZ, Y. **Criptografia de Curva Elíptica Bitcoin (ECDSA) explicada em detalhes (Desvendando os segredos do Bitcoin)**. Steemit. Disponível em <https://steemit.com/cervantes/@ydavgonzalez/criptografia-de-curva-eliptica-de-bitcoin-explicada-al-detalle-desentranando-lo-secretos-de-bitcoin> Acesso em 10 de junho de 2018.

LIMA, B.H.N., HITOMI, F.A.C. e OLIVEIRA, G.S. **Aplicação da tecnologia blockchain em ambientes corporativos**. Fatec Antônio Russo –São Caetano do Sul. Fasci-Tech. 2018.

MARTINS, T.F. **Prova de existência de arquivos digitais utilizando a tecnologia Blockchain do protocolo Bitcoin**. Universidade Federal do Rio Grande do Sul, Porto Alegre, 2018.

NAKAMOTO, S. **Bitcoin: A Peer-to-Peer Electronic Cash System**. 2009. Disponível em <https://bitcoin.org/bitcoin.pdf> Acesso em 30 de março de 2018.

OLIVEIRA, J.G. **Curvas Elípticas sobre Corpos Finitos e Criptografia de Chave Pública**. Universidade Federal do Espírito Santo. I Colóquio Regional da Região Centro-Oeste, 3 a 6 de novembro de 2009. Universidade Federal de Mato Grosso do Sul.

PAVÃO, S. **Criptomoeda: o que é e como usar**. Psafe Blog. Disponível em <http://www.psafe.com/blog/o-que-criptomoeda/> Acesso em 12 de março de 2018.

PIRES, T.P. **TECNOLOGIA BLOCKCHAIN E SUAS APLICAÇÕES PARA PROVIMENTO DE TRANSPARÊNCIA EM TRANSAÇÕES ELETRÔNICAS**. Universidade de Brasília, 2016.

RYKWALDER, E. **A matemática por trás do Bitcoin**. Bitcoin On Air. Disponível em <https://pt.bitcoinonair.com/math-behind-bitcoin> Acesso em 29 de maio de 2018.

SILVA, G.A.B. e RODRIGUES, C.K.S. **Mineração individual de *bitcoins* e *litecoins* no mundo**. Faculdade de Tecnologia e Ciências Sociais Aplicadas, Brasília. XVI Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais. 2016.