Ministério da Educação
Universidade Tecnológica Federal do Paraná
Pró-Reitoria de Pesquisa e Pós Graduação

Projeto de Pesquisa

Área de Conhecimento (CNPq)

a) Ciência da Computação: 1.03.00.00-7

b) Sistemas de Computação: 1.03.04.00-2

c) Teleinformática: 1.03.04.04-5

Estudos Sobre Aplicação de Computação Ubíqua na Tecnologia de Criptomoedas

Coordenador: Prof. Dr. Ricardo Fernandes da Silva

Colaboradores: Prof. Dr. Emilson Ribeiro Viana Junior

Prof. Dr. Walmor Cardoso Godoi

Universidade Tecnológica Federal do Paraná (UTFPR)

Departamento Acadêmico de Física (DAFIS)

Av. Sete de Setembro, 3165, Rebouças, Curitiba-PR

CEP 80230-901

CAMPUS Curitiba, Setembro 2017

1. Caracterização do Problema

Computação ubíqua pode ser definida como, algo que se utiliza de componentes computacionais, hardware e/ou software, e se comporta de forma pró-ativa, onipresente, imperceptível e natural, de tal forma que os indivíduos convivam e interajam com os computadores sem mesmo perceber [1]. Uma tecnologia computacional, para enquadrar-se na computação ubíqua, deve ser excepcionalmente amigável, para que possa assim ser definida.

O Bitcoin surgiu, no final de 2008, ele tinha como um de seus objetivos, a inclusão em algum sistema financeiro, uma população de aproximadamente 2 bilhões de pessoas no globo que eram desbancarizadas [2]. Esse número ainda continua alto, estima-se que ainda 48% da população mundial adulta, ainda é desbancarizada, ou seja, sem acesso ao crédito por falta de cadastro, pré-requisitos das instituições bancárias como residência fixa, renda e garantias [3]. No Brasil 32% da população adulta não tem uma conta bancária e 53% das médias e pequenas empresas não têm acesso à crédito [4] Pode-se então afirmar, que o Bitcoin não atingiu ainda o seu objetivo, de incluir no sistema pessoas desbancarizadas de forma contundente, porém é inegável seu valor como tecnologia disruptiva e inovadora. Acredita-se que essa "falha" do Bitcoin se deu por não ser um produto tecnológico de fácil utilização, como ocorre com as outras criptomoedas.

A rede subjacente de diversas criptomoedas, utiliza o conceito de blockchain, que é um *software* contendo o arquivo de todas as transações da história, e que encontra-se instalado em diversos computadores ao redor do globo. Este arquivo é incrementado a todo momento em que um novo bloco deve ser adicionado a rede, e todos os computadores com este software devem concordar, por meio de uma lógica de consenso, que o referido arquivo é válido e assim aceitam a sua inclusão no blockchain. Fazendo com que desta forma a rede valide a inclusão daquele arquivo e funcione sem a necessidade de um terceiro de confiança [2].

Desde o final de 2008 com a divulgação do White paper do Satoshi Nakamoto [2] a rede bitcoin sem desenvolveu, sem a comunidade acadêmica dar a devida atenção a sua invenção e as possíveis aplicações desta tecnologia, principalmente o blockchain. Pode-se notar o crescente interesse sobre a tecnologia blockchain pela comunidade acadêmica quando faz-se uma busca pelas palavras-chave cryptocurrency e blockchain na plataforma ScienceDirect, esta constatação pode ser observada na figura 1 abaixo.

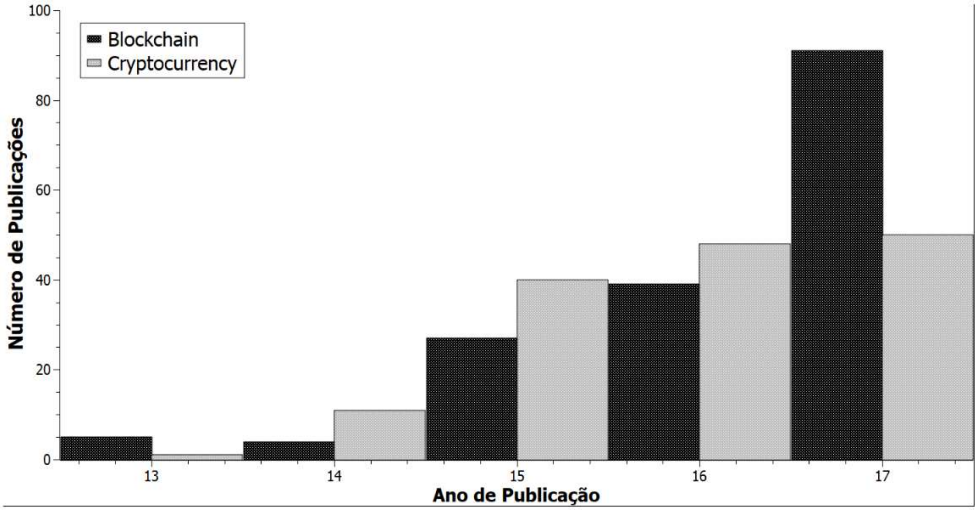

Figura 1 - Número de Publicações anual com a palavra chave Blockchain e Cryptocurrency

As criptomoedas, como o Bitcoin, Ethereum, Monero, Litecoin, Zcach, Dash entre outras não são uma tecnologia que se enquadre na ubiquidade diretamente, pois em geral para o usuário iniciar qualquer operação financeira com Criptomoedas ele se depara com um grande número de termos técnicos que não são usuais para seu cotidiano. Termos como, criptografia de chave dupla, carteira digital, *exchange*, mineração, *polls* de mineração, prova de trabalho, *blockchain*, etc.

O objetivo principal deste estudo é encontrar formas de tornar o bitcoin (ou o acesso a ele por meio de outras criptomoedas) o mais natural possível aos indivíduos bancarizados ou não, acredita-se que para atingir este objetivo final a computação ubíqua seja um caminho a ser trilhado.

2. Objetivos e Metas

- Desenvolvimento de material específico de “introdução ao uso de Bitcoin no dia-a-dia” guiando futuros usuários.
- Verificar a viabilidade, de implementar soluções de simples utilização para o usuário final, com as soluções financeiras disponíveis, pela utilização das tecnologias de criptomoedas.
- Desenvolvimento de um software *user friendly* para transferência ponto a ponto P2P entre usuários, de preferência em plataforma *mobile* (Android/iOS).
- Desenvolvimento *de hardwares* específicos para transações bitcoin na Lightning Network [5].

3. Métodos e Procedimentos

O desenvolvimento do trabalho consistirá na execução dos seguintes passos:

1) Organização de um grupo de estudos sobre os temas relevantes e necessários para o desenvolvimento do projeto;
2) Organização e realização de palestras, workshops e eventos relativos ao tema de criptomoedas e *blockchain*;
3) Desenvolvimento de sistemas com ferramentas computacionais e hardware para simulações e aplicações com Criptomoedas e *blockchain*;
4) As ferramentas ficarão disponíveis em um repositório público na plataforma github.

4. Resultados e/ ou produtos esperados

- Compreensão dos termos e técnicas utilizados para criação e desenvolvimento das criptomoedas;
- Formação de grupo de profissionais aptos a desenvolver soluções, para tornar possível que as criptomoedas se tornem ubíquas;

- Parcerias com empresas de tecnologia e financeiras.

- Ferramenta computacional e hardware *user friendly* para criptomoedas.

5. Recursos e equipamentos disponíveis

Para realização desses estudos serão utilizados:

- Auditórios;
- Salas de aulas;
- Computadores;
- Servidores de rede;
- Cluster computacional e
- Laboratórios de informática disponíveis no departamento de Física.

Obs.: Nenhum recurso desta Universidade será utilizado para realização de mineração POW (Proof of Work).

6. Riscos e Dificuldades

Os riscos do projeto são:

- Falta de recursos de hardware e rede para o desenvolvimento da pesquisa.
- Falta de envolvimento de alunos de iniciação científica.

7. Justificar a escolha da modalidade no processo de submissão

Este trabalho caracteriza-se como um projeto de pesquisa por contemplar os requisitos de PESQUISA APLICADA na área de Econofísica, Física Computacional, Criptografia, Ciência e Engenharia da Computação, Eletrônica, Teleinformática, enfim uma confluência de diversas áreas do conhecimento atuando em conjunto para facilitar o acesso e a compreensão das criptomoedas .

8. Referências Bibliográficas

[1] SILVA, E. et al. Computação Ubíqua – Definição e Exemplos. Revista de Empreendedorismo, Inovação e Tecnologia, Passo Fundo, v. 2, n. 1, p. 23-32, dez. 2015. ISSN 2359-3539. Disponível em: <https://seer.imed.edu.br/index.php/revistasi/article/view/926/739>. Acesso em: 23 ago. 2017. doi:http://dx.doi.org/10.18256/2359-3539/reit-imed.v2n1p23-32.

[2] NAKAMOTO, S. Bitcoin: A Peer-to-Peer Electronic Cash System, Novembro de 2008 – Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em 13 set. 2017

[3] OLIVEIRA, L. O capital dos pobres: Endowment Fund como inovação para a formação de poupança de longo prazo no Banco Palmas. Monografia submetida ao curso de Ciências Econômicas da Universidade Federal de Santa Catarina. 2016. Disponível em: <

https://repositorio.ufsc.br/xmlui/bitstream/handle/123456789/167562/Monografia%20do%20Lucas%20Oliveira.pdf?sequence=1&isAllowed=y>. Acesso em: 23 ago. 2017.

[4] McKinsey Global Institute - DIGITAL FINANCE FOR ALL: POWERING INCLUSIVE GROWTH IN EMERGING ECONOMIES - September 2016. Disponível em: <https://goo.gl/Ebq2O7> Acesso em: 24 ago. 2017

[5] Poon J., Dryja T. The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments, Janeiro de 2016 – Disponível em: <https://lightning.network/lightning-network-paper.pdf>. Acesso em 13 set. 2017