INSTITUTO DE EDUCAÇÃO SUPERIOR DA PARAIBA – IESP

SISTEMA DE INFORMAÇÕES

JOSÉ PIRES DA SILVA JUNIOR

RELAÇÕES DE CONSUMO ATRAVÉS DE BITCOIN

JOÃO PESSOA

2017

JOSÉ PIRES DA SILVA JUNIOR

RELAÇÕES DE CONSUMO ATRAVÉS DE BITCOIN

Trabalho de Conclusão de Curso apresentado ao Instituto de Educação Superior da Paraíba, como exigência para obtenção parcial do título em Bacharel de Sistemas de Informação

JOÃO PESSOA

2017

S586R **SILVA JUNIOR, JOSÉ PIRES DA**

Relações de consumo através de bitcoin / José Pires da Silva Junior. – João Pessoa, PB: [s.n], 2017.

48p.

Orientador: Prof. Ms. Hercílio de Medeiros Sousa. Monografia (Graduação em Sistemas de Informação) – Instituto de Educação Superior da Paraíba - IESP.

RELAÇÕES DE CONSUMO ATRAVÉS DE BITCOIN

Trabalho de Conclusão de Curso apresentado ao Instituto de Educação Superior da Paraíba, como exigência para obtenção parcial do título em Bacharel de Sistemas de Informação

Aprovada em: _____de_____de 2017.

BANCA EXAMINADORA

_____

Prof. Me. Hercilio de Medeiros Sousa (orientador)
Instituto de Educação Superior da Paraíba

_____

Prof. XXXXXX
Instituto de Educação Superior da Paraíba

_____

Prof. XXXXXX
Instituto de Educação Superior da Paraíba

DEDICATÓRIA

Dedico este trabalho aos meus pais que me deram a vida, minha namorada, aos meus familiares e amigos que de forma direta ou indireta me ajudaram a vencer as etapas deste desafio.

AGRADECIMENTOS

A minha família que sempre me apoiou em todos os momentos do curso, em especial a minha mãe e ao meu pai que sempre me apoiaram em todas as minhas decisões. Quero agradecer também a minha namorada que teve muita paciência comigo nesse fim de período, e ao meus amigos e colegas que de maneira indireta também fizeram parte do desenvolvimento desse trabalho.

Agradecer também a faculdade Iesp por me proporcionar essa experiência, e ao meu professor orientador Hercílio de Medeiros e também ao nosso coordenador Marcelo.

RESUMO

O seguinte trabalho analisa como as pessoas interagem com a inovação e o conhecimento delas a respeito de moedas virtuais e suas transações, que ano de 2008 marcou o surgimento das moedas virtuais, e que mostrou ao mundo através de um artigo uma inovação para a economia mundial, o conteúdo falava a respeito de uma no moeda totalmente digital e não centralizada, é independente de qualquer banco mundial, a moeda chamada bitcoin. Que no ano seguinte passou a funcionar e estar fazendo muito sucesso. Atualmente já existe diversas outras moedas, mas a bitcoin é a de maior destaque, com valores absurdos e um sistema de bloco que inspira o desenvolvimento de várias outras moedas, o bitcoin vem mexendo muito com as pessoas e os governos com o seu surpreendente crescimento.

Palavras-chave: Bitcoin, economia, bloco, transação

LISTA DE FIGURAS

LISTA DE GRÁFICO

SUMÁRIO

1 INTRODUÇÃO

Bitcoin é uma primeira implementação do que se pode chamar de cripto-moeda, apresentando se em 1998 e relatada por Wei Dai, os bitcoins e nada mais que uma rede consensual com uma nova possibilidade de pagamento, não centralizada, onde os usuários gerenciam o sistema, assim não necessitando de intermediadores, e sendo assim também uma nova moeda totalmente digital.

A rede de bitcoin consiste de um software livre(opensource), já que o bitcoin consiste de um software com seu código aberto, isso atraí os olhos dos hacker's, e dessa maneira o software não poderia estar vulnerável.

A facilidade de pagamentos e suas transações são em tempo real independente de hora, dia ou local, essa facilidade de poder efetuar transações e pagamentos atrai os olhares de empresas, nações e consumidores, já que o mesmo tem tempo de funcionamento a todo instante de maneira ágil e segura.

É possível que esse software venha fazer parte das transações online de uma maneira muito mais abrangente, facilitando a vida de milhões de pessoas, de países etc, fazendo essa moeda digital girar e assim também influência na economia, global, continental e regional.

Com o surgimento do bitcoin e sua tecnologia da blockchain que falaremos sobre no desenvolver desse trabalho, fez com que fosse surgindo novas outra moeda seguindo a ideia dos bitcoins em fazer transações, assim como também moeda com um desenvolvimento diferenciado da blockchain e uma ideia um pouco distinta, com um poder de efetuar qualquer tipo de transação financeira independentemente do tamanho da mesmo, assim atingindo até as micro transações, mostrando a viabilidade da mesma e sem nenhum custo pela as mesma.

Mas de que maneira os bitcoins poderia impactar a economia mundial, será que essa nova forma de transação online poderia substituir pagamentos como os cartões de uma maneira mais segura, e de uma maneira não burocrática já que o mesmo não depende de terceiros para efetuar as transações e tão pouco cobrar taxas abusivas que são cobradas através dos bancos e empresas que terceirizam esses meios de transações online de cartões.

A tecnologia de moedas online que efetivamente vem funcionando de alguns anos pra cá vem se destacando cada vez mais, instituições, empresas e países estão de olho, vendo as possibilidades de inovação que as mesmas podem trazer, e os benefícios para as nações que ao aderir poderá trazer.

Dessa maneira vamos discutir a viabilidade dessa moedas que vem surgindo, como também a confiabilidade das mesmas, diante de moedas distintas mas que podem ou não ser mais confiáveis e até mesmo ter um foco diferente de uso e algumas implementações que faram com que a confiabilidade seja realmente efetiva.

2.1 OBJETIVOS

2.2.1 OBEJETIVO GERAL

Demonstrar como os Bitcoins podem impactar na economia e no que isso pode influenciar nos pagamentos eletrônicos na vida das pessoas.

2.2.2 OBJETIVOS ESPECÍFICOS

- Demonstrar a importância de bitcoins no mercado digital.

- Discutir a utilização dos bitcoins nas transações financeiras online, e de que forma isso pode otimizar a vida dos usuários.

- Discutir a viabilidade e a confiabilidade das transações com bitcoins e suas vantagens entre as demais tecnologias atuais.

- Analisar os impactos econômicos e sócias da inserção dos bitcoins no mercado.

3 BITCOIN

Bitcoin é a primeira moeda digital, criado em 2008 por um programador de nome Satoshi Nakamoto, é uma moeda assim como o Real, o Dólar e o Euro, de maneira que o bitcoin é uma moeda exclusivamente eletrônica. Até o seu surgimento, transações online eram feitas atrás de terceiros, já que os bancos e empresas de cartões sempre intermediavam essas transações, de maneira que elas teriam regulamentações e taxas de serviços que estariam sendo ofertadas. O fato de a moeda ser eletrônica faz com que os bancos e governos não as regulem. Uma forma de fazer isso foi criando o sistema de maneira não centralizada, assim não dependendo de terceiros para mediar essas transações. A transações do Bitcoin funciona de maneira ponto-a-ponto(peer-to-peer) direta, instantânea e sem burocracias, e assim tornando os usuário da transação os próprios intermediários.

> Se Maria quisesse enviar 100 u.m.(unidade monetária) ao João por meio da internet, ela teria que depender de serviços terceirizados como o PayPal ou MasterCard. Intermediários como o PayPal mantêm um registro dos saldos em conta dos clientes. Quando Maria enviar 100 u.m. ao João, o PayPal debita a quantia em sua conta, creditando a na conta de João. Sem tais intermediários, um dinheiro digital poderia ser gasto duas vezes. (Ulrich, 2014, p. 17)

Em bitcoin todas as transações são registradas na blockchain, a blockchain seria uma espécie de livro de registros, público e que nele consiste o registro histórico da transações ocorridas, assim sendo um banco de dados de registro de transações financeiras do bitcoin. Como o Ulrich (2014) descreve que o valor do bitcoin em reais e estabelecido assim como outras moedas em mercado aberto e estabelecido em casas de câmbio entre as diferentes moedas mundiais.

As transações são feitas de forma criptografada, a criptografia das transações são feitas através de duas chaves, chave primaria e chave estrangeira. A chave pública, como o próprio nome já diz ela é pública e consequentemente compartilhada, já a chave privada e mantida em sigilo.

> Todas as partes podem acessar a chave pública. Os dados criptografados por meio de uma chave pública só podem ser descriptografadas com o usa da chave privada. (Reisswitz, 2008, p. 28)

Assim os dados criptografados com a chave pública só são descriptografados com o uso da chave privada.

A criptografia da chave pública fornece a todos os computados da rede as transações da rede verificados e atualizados em forma de registros impossibilitando as fraudes e o duplo gasto.

Como foi visto a rede bitcoin funciona de forma não centralizada, e não dependente de uma autoridade para verificar as transações e nem a criação monetária. A rede depende do poder de processamento computacional para a realização dos registros e das transações. Os usuários que se dispõem a esse tipo de processo computacional solucionando complexos problemas matemáticos que vai a fazer verificação de transações na blockchain são chamados de mineradores, os minerados como recompensa da sua disponibilização recebem bitcoin recém criados. O bitcoin faz uma busca por combinações por um tipo de padrão, quando a combinação ocorrer, que o minerador receberá sua bonificação de bitcoins, e o tamanho dos bitcoins são reduzido a medida que eles vão sendo minerados.

> Uma vez que um número predeterminado de moedas entrou em circulação, o incentivo pode transitar inteiramente para taxas de transação e ser completamente livre de inflação. (Nakamoto, 2008)

A moeda foi feita pensada de maneira que fosse real assim como os metais precioso como o ouro, por tanto existe um número limite de bitcoin a ser minerada, pois existe um quantidade limite de bitcoin, quantidade essa de 21 milhões de bitcoins. Segundo Nakamoto (2008) se estima que os mineradores colherão o último 0,00000001 de bitcoin no ano de 2140 e que a potência de mineração chegar a níveis muito elevados a dificuldade aumentará, que para encontrar o último bitcoin será uma empreitada digital desafiadora.

De maneira que os mineradores não deixassem de contribuir com as transações financeiras, com seus processamentos para afim de verificações dessas transações os mesmo serão recompensados com taxas de serviços, ao invés de novos bitcoin minerados, para continuar a incentivar os mineradores após a extração do último bitcoin.

3.1 CRIPTOGRAFIA

O conceito principal do desenvolvimento do bitcoin era a inexistência de um intermediador, sem bancos, sem empresas de cartões ou sem governo, porém existem problemas na moeda, problemas esse de segurança, de que não ocorra roubo de moedas ou que alguém venha a passar por outra pessoa.

Dessa maneira é utilizado a criptografia, a criptografia é nada mais que uma maneira de ocultar as informações de forma codificada, que apenas os emissores e os receptores tenham como decifrar a mensagem transmitida.

A criptografia converte dados legíveis em algo sem sentido, com a capacidade de recuperar a partir desses dados sem sentidos (Burnett & Paine, 2002, p. 1)

Na criptografias existes uns tipos das mesma, porém no caso de bitcoin é utilizada a mais segura que é a Criptografia Assimétrica, que será falada nesse próximo tópico.

3.2 CRIPTOGRAFIA ASSIMÉTRICA

A criptografia assimétrica é um tipo de criptografia das que foram desenvolvidas, ela foi desenvolvida na década de 1970, em que os comunicadores portaram duas chaves diferentes, uma chave pública e outra chave privada, ela também é conhecida pelo nome de criptografia de chave pública.

“Conhecida como ‘chave pública’, a chave assimétrica trabalha com duas chaves: uma denominada *privada* e outra denominada *pública*. (Burnett & Paine, 2002)

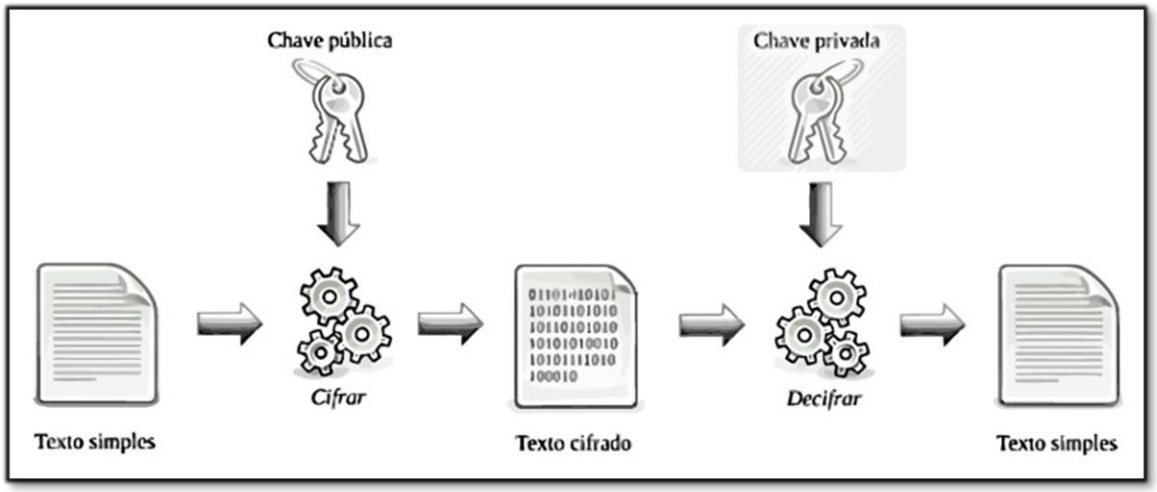

Figura 1- Criptografia assimétrica

Fonte: Daniel Fernando Pigatto,2012

Como podemos ver na figura a cima, a chave pública é utilizada para a cifragem do texto, que é transmita pela rede, é o receptor com a chave privada que poderá decrifrar essa cifragem assim tendo a permissão de saber o conteúdo da mensagem.

> A chave assimétrica trabalha com duas chaves: uma denominada *privada* e outra denominada *pública*. Neste método, um emissor deve criar uma chave de codificação e enviá-la ao receptor. Essa é a chave pública. Uma outra chave deve ser criada para a decodificação. Esta, a chave privada, é secreta. (Alecrin, 2009)

3.3 BLOCKCHAIN

Na área dos bitcoins, a blockchain é uma estrutura de dados que é mantida o arquivo em cada nó, de forma não centralizada que representa um registro das transações financeiras. Cada uma das transações é digitalmente assinada para que a autenticidade possa garantir que ninguém adulterou, assim garantindo a integridade da transação. Ao fazer uma nova transação, ou menos uma correção de uma transação existente, normalmente os nós de implementação dentro da blockchain devem executar algoritmos e, avaliar o bloco do blockchain de forma individual para assim chegar a concordância de que o histórico e a assinatura são

validos, dessa maneira permitindo uma nova transação no registro e adicionando um novo bloco a cadeia de transação.

> Podemos qualificar o blockchain como um grande livro-razão, único e compartilhado por todos os participantes do sistema, no qual as transações são registradas de forma irreversível – quanto mais antigo o bloco, mais computacionalmente impraticável de reverter são as operações. (Ulrich,2015)

Entretanto um bloco não contém apenas as informações incluídas neles e as do bloco anterior, mas também a solução da Prova de Trabalho(Proof-of-work) necessário para ser aceita pelos demais participantes da rede. Para que o mecanismo funcione da seguinte maneira as transações são feita de uma maneira inovada que a bitcoin proporciona, requerendo que as transações sejam feitas de forma pública.

> Uma prova de trabalho é um pedaço de dados que foi difícil, para produzir, de modo a satisfazer certos requisitos. Deve ser trivial verificar se os dados satisfazem as referidas exigências. Produzir uma prova de trabalho pode ser um processo aleatório com baixa probabilidade, de modo que um monte de tentativa e erro é exigido em média antes de uma prova válida de trabalho é gerado. Bitcoin usa a prova Hashcash do trabalho. (Ganhe seu primeiro Bitcoin, Conheça tudo sobre a moeda, 2017)

Embora não se conheçam as partes transacionadas, as transações ocorrem de maneira a serem validadas e registradas por qualquer usuário, incrementando a corrente a medida que mais blocos vão sendo agregados.

As transações as quais são registradas em cada bloco da blockchain, é as transações ocorridas pelos usuários e a criação de novos bitcoins pelos mineradores.

> O bitcoin é, portanto, um registro em ordem cronológica de todas as transações que ocorrem na rede e foram compiladas e validadas pelos mineradores. O blockchain é público, único, replicado e compartilhado pelos participantes do sistema. Sua manutenção e atualização ocorrem de forma centralizada e voluntaria, sendo a emissão de novos bitcoins o incentivo dado a quem se dedica a tarefa de mineração (Ulrich, 2015)

Os bitcoins existem apenas como registros na blockchain. A blockchain existe para registra as transações dos usuários e registras as propriedades dos mesmos. Assim como foi dito por Ulrich (2015) que um depende do outro, a tecnologias engloba ambas as partes.

3.4 MINERAÇÃO

O bitcoin é um moeda criptografada, que assim como as moedas oficiais, atendente as necessidades, porém essa moeda não é emitida por nenhuma autoridade de nenhum pais, é uma moeda totalmente digital e descentralizada. Dessa maneira existe uma forma de se criar esse bitcoins, que tem uma numeração máxima, mas que o próprio programa vai calibrando a dificuldade conforme a emissão das moedas e feita.” a quantidade existente no mercado é rigorosamente controlada para evitar que sua cotação desabe.” (Piropo, 2014)

Para que o sistema bitcoin funcione, é necessário processar e validar as transações, para isso é utilizado uma rede de computadores conectados à internet que formam a rede descentralizada do bitcoin. Qualquer pessoa pode se juntar a rede e agregar poder de processamento a ela, que será utilizado para processar as validações já que o sistema não possui um dono. Com esse sistema de mineração os mineradores recebem bitcoins como incentivo através de taxas, para efetuar o processamento e validação das transações.

> Qualquer pessoa é capaz de obter bitcoins sem comprá-los de outros usuários, baixando e executando o programa de mineração de bitcoins. Milhares de computadores pessoais atualmente computam a base de codificação bitcoin, o sistema recompensa bitcoins a qualquer mineiro que passe a calcular a própria cadeia de blocos. (Kaplanov, 2012, p. 119)

Assim não existindo uma central de gerenciamento, voluntários da rede bitcoin que solucionam problemas matemáticos, o mesmo que decifrar o problema será recompensado com bitcoin e dessa maneira a rede continua a operar. Assim computadores pessoais se tornam uma maneira difícil de se beneficiar com a mineração, de acordo com que a dificuldade dos problemas matemáticos tem a tendência de aumentar e ter um tempo de execução para efetuar os mesmos.

> Para compensar o aumento da velocidade do hardware e o interesse variável em executar os nós ao longo do tempo, a dificuldade de prova de trabalho é determinada por uma média móvel direcionada a um número médio de blocos por hora. Se eles são gerados muito rápido, a dificuldade aumenta. (Nakamoto, 2008)

De acordo com o que Kaplanov (2012) fala, que pelo fato de ser difícil um computar pessoal revolver os cálculos, mineradores se juntam para combinar o poder de processamento, assim minerando de forma agrupada, dividindo o problema em partes e resolvido por vários computadores.

3.5 TRANFERÊNCIA

A transferência de bitcoins é simplesmente uma passagem de moedas digitais de um endereço para o outro na rede, logo a baixo temos uma figura que mostra o funcionamento que é bem simples:

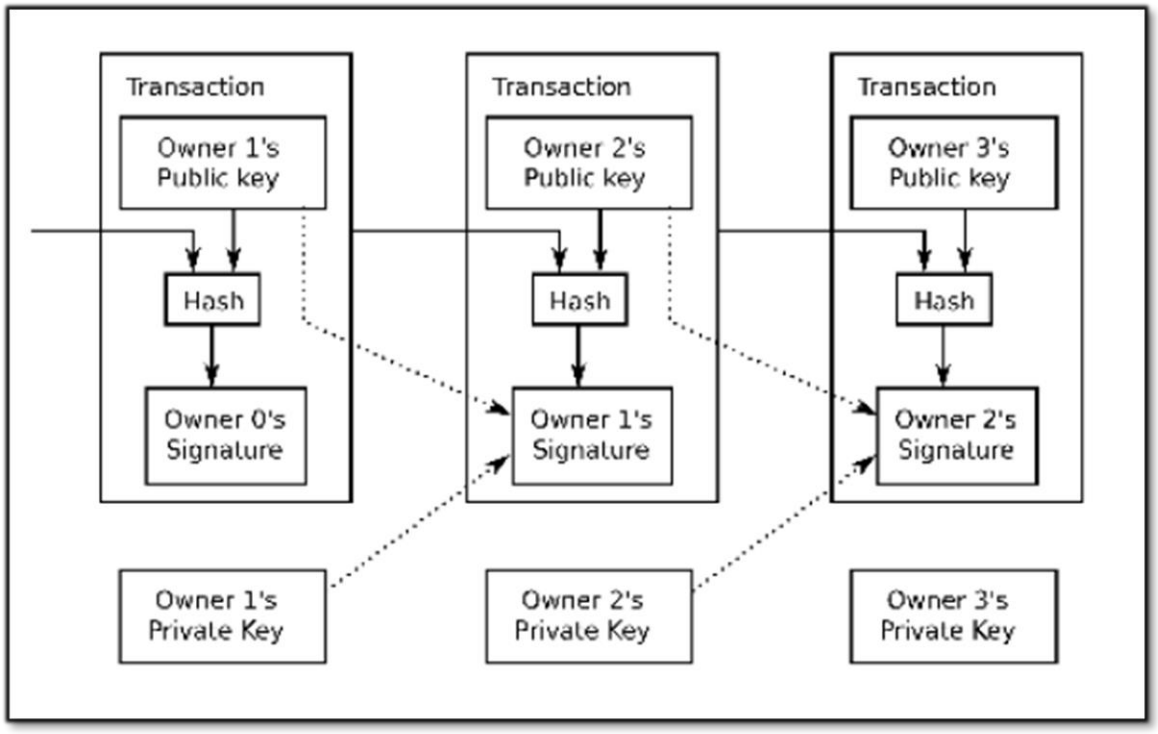

Figura 2 - Tranferência de Bitcoins

Fonte: Discas para Computador, sem data.

Como podemos ver na figura a cima e como Silva (2014) explica, que o processo de transação tem como entrada o hash da transferência anterior e a chave pública do próximo dono e que ambos passam por um processo de soma e por fim são assinados com a chave privada do dono atual, e o portador da moeda envia uma mensagem assinada por broadcast atrás da rede.

3.6 WALLETS

As wallets são nada mais nada menos que as carteiras bitcoins, essas carteiras tem como objetivo de guardar as moeda bitcoins, tal qual enviar e receber moedas bitcoins, e a proteção das chaves dos usuários.

> Suas principais finalidades consistem em: envio e recebimentos de Bitcoins, geração de endereços, gerenciar saldos, proteger as chaves dos usuários por meio de senhas e criptografia dos dados. (Silva, 2014, p. 232)

Hoje em dia existe alguns tipos de wallets, os mesmos tem suas funções parecidas, porém sua utilização difere, podendo está diretamente conectado à rede ou não, como veremos, já que hoje temos software wallets, paper wallets e web walles que descreveremos brevemente abaixo cada um:

3.6.1 SOFTWARE WALLETS

Essa primeira carteira funciona como qualquer outra, você irá receber o endereço bitcoin, poderá enviar e receber bitcoins, no entanto é necessário a instalação da mesma em seu dispositivo, seja ele um computador, celular ou tablet, com disponibilidade para android, IOS e Windows.

> Os softwares wallets são programas que podem ser instalados nos dispositivos do usuário capazes de se conectar diretamente com a rede Bitcoin, sincronizando a Blockchain localmente, e permitem a manipulação da moeda. (Silva, 2014, p. 232)

Logo abaixo podemos ver a imagem de uma software wallet:

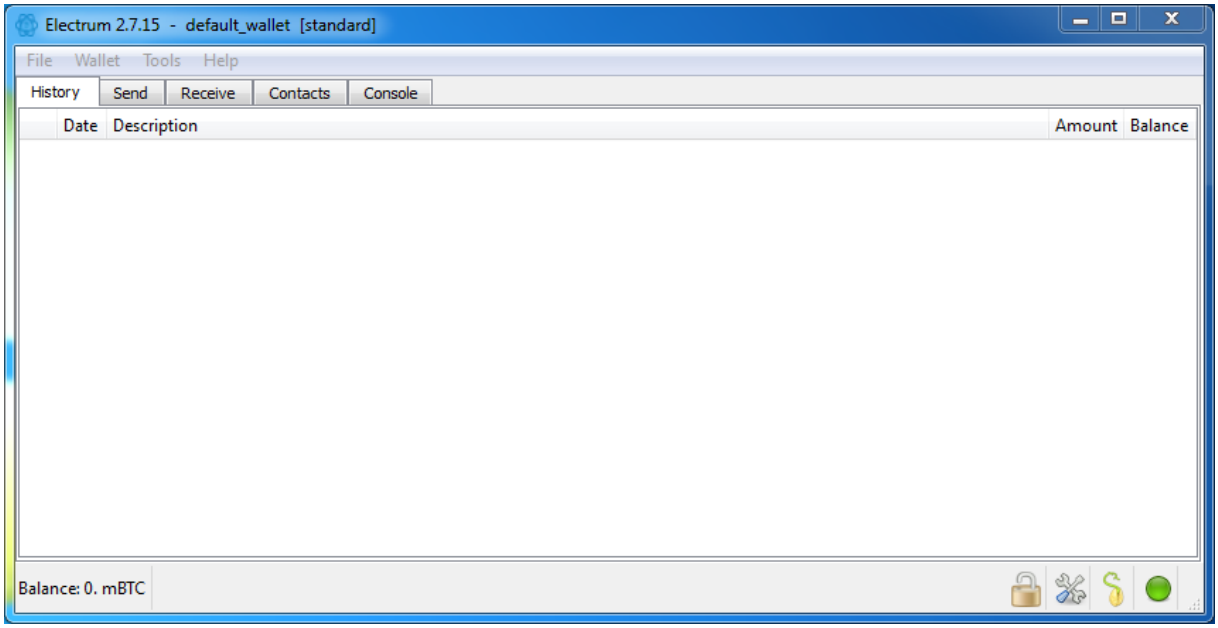

Figura 3 Software Carteira Electrum

Fonte: CoinGat Blog,2016.

3.6.2 WEB WALLETS

São carteiras online, esses tipos são acessados através dos próprios navegadores, essas carteiras são armazenadas em servidores dos provedores do serviço, dessa maneira facilitando o acesso em qualquer lugar do mundo tendo acesso à rede.

> Web wallets são sites que disponibilizam o mesmo serviço de software wallet, porém com alguns recursos limitados, a depender de cada site, e, normalmente, cobram taxas de manutenção de contas e transações. Sua vantagem é o fornecimento de segurança e gerenciamento para as chaves privadas dos usuários e desnecessidade de ter que sincronizar com a blockchain. (Silva, 2014, p. 233)

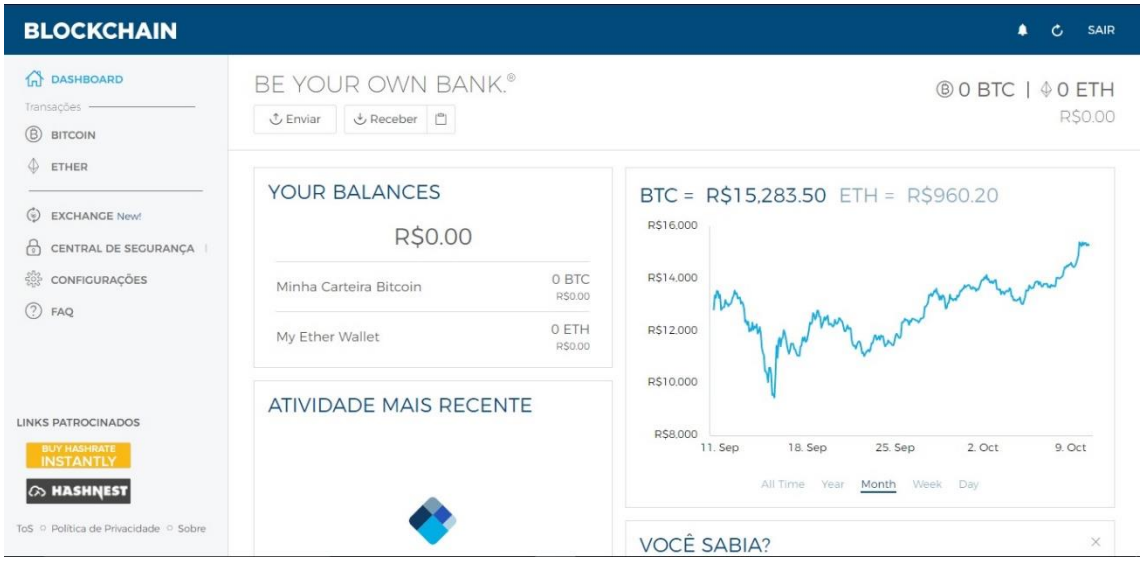

Figura 4 Carteira Blockchain

Fonte: Blockchain,2017.

3.6.3 PAPER WALLETS

Essa carteira pode ser chamada de carteira de papel, já que a mesma é feita em papel impresso, ela é uma carteira que você cria um endereço bitcoin e uma chave para você ter acesso, é um tipo de carteira fora da internet.

> Paper wallet são impressões em papel dos endereços Bitcoin mais o par de chaves privada e pública. É considerada um meio off-line de gerenciamento de chaves que se aproxima da noção de moeda tradicional. (Silva, 2014, p. 234)

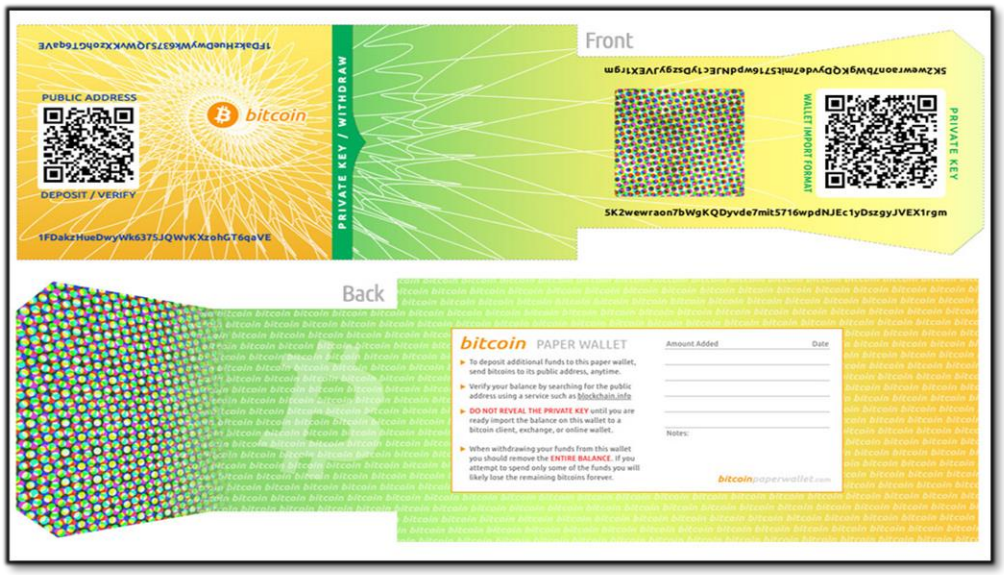

Figura 5 Carteira de Papel

Fonte: Bitcoin Paper Wallet,2017.

3.7 EXCHANGE

A Exchange permite aos usuários a compra e venda de moedas digitais, as exchanges funcionam como casas de câmbio.

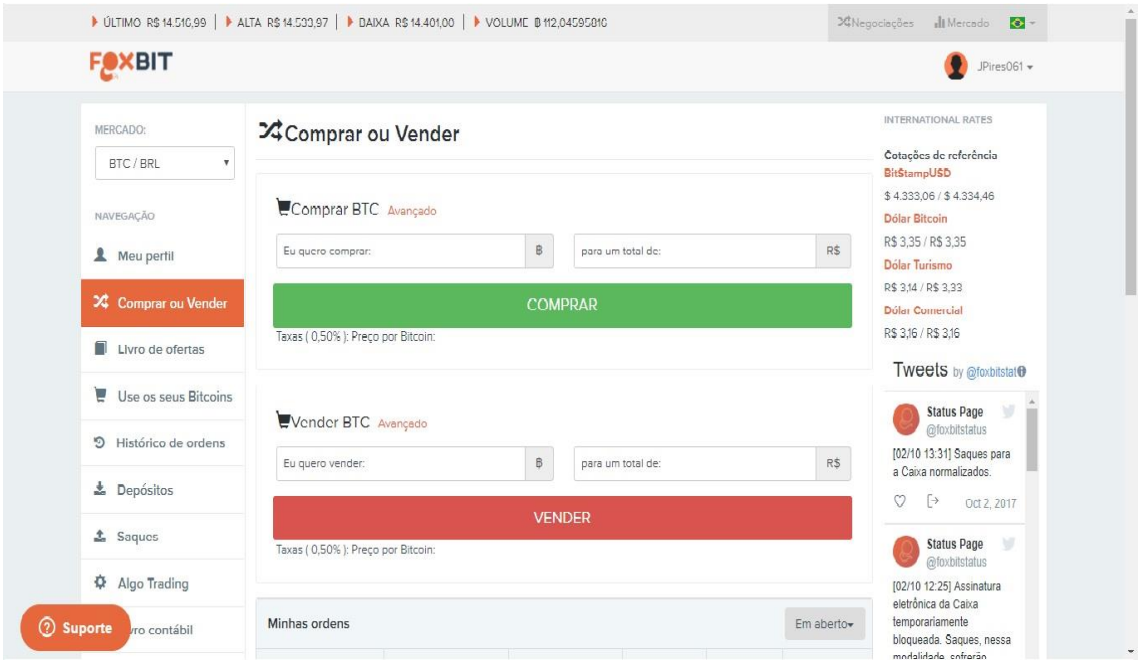

Figura 6 Exchange Foxbit

Fonte: Foxbit,2017

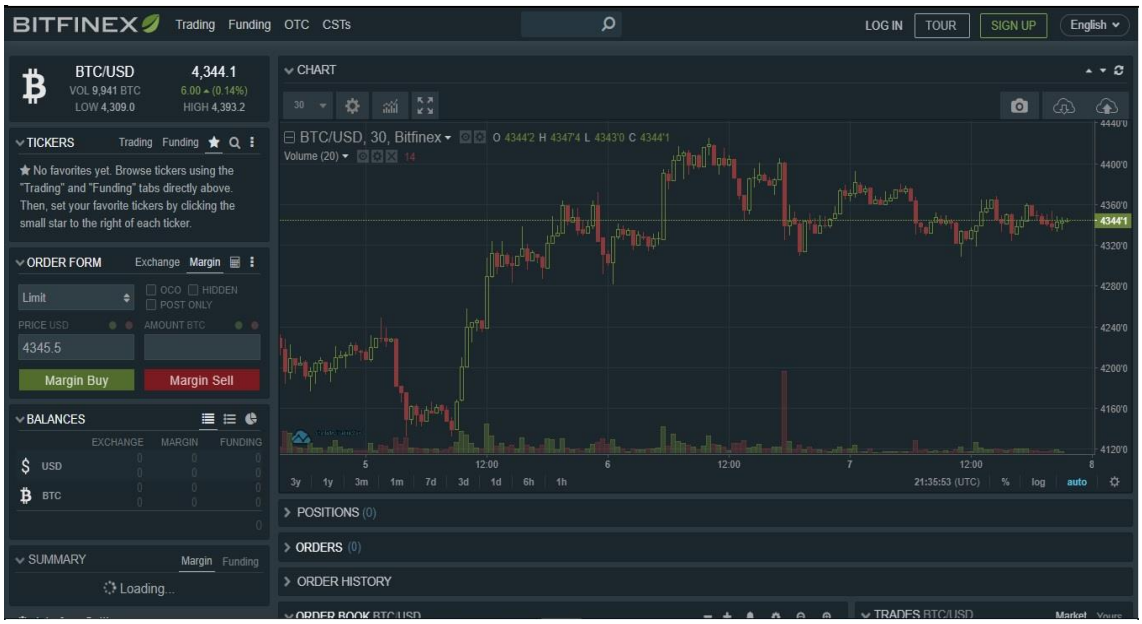

Figura 7 Exchange Bitfinex

Fonte: Bitfinex,2017

> O seu funcionamento é idêntico a uma casa de câmbio, ou seja, uma parte troca o bitcoin por moeda nacional com a intermediação da Exchange, que sobre a operação cobra taxa. (Silva, 2014, p. 234)

3.8 O QUE DETERMINA O PREÇO DOS BITCOINS

O preço dos bitcoins varia de acordo com a oferta e a demanda. A medida que a demanda dos bitcoins aumenta, o valor sobe também, assim como a demanda dos mesmo caem o valor deles também tendem a cair. Há um número como Silva (2014) relata limitado de bitcoins em circulação e novos bitcoins são criados de maneira previsível e decrescente, o que mostra que a demanda deve seguir no mesmo no nível atual e manter estável o valor.

Logo abaixo podemos ver um gráfico mostrando as mudanças do valor dos bitcoins no decorre de janeiro de 2013 até o mês de janeiro do ano de 2015:

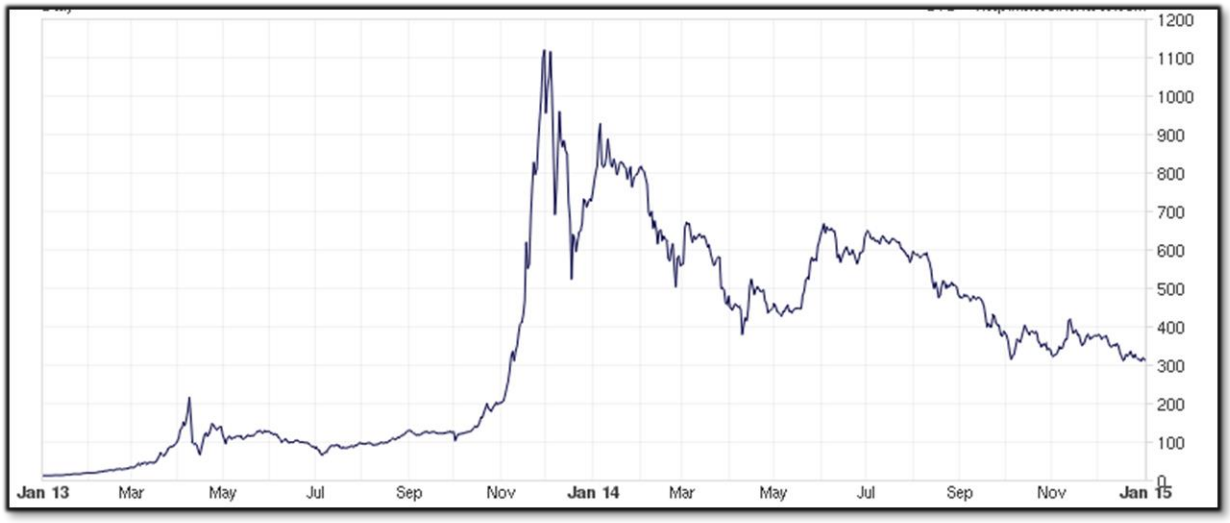

Gráfico 1 - Variação de Preço

FONTE: Bitcoin.org, 2017

3.9 SEGURANÇA

A tecnologia bitcoin, o protocolo e a criptografia tem um registro forte de segurança e a rede bitcoin é provavelmente o maior projeto de computação distribuída do mundo. A vulnerabilidade mais comum do bitcoin é o erro do usuário. Os arquivos de carteira de bitcoin que guardam as chaves privadas necessárias, podem ser apagadas, roubadas ou perdidas. Isto é bem parecido com dinheiro tradicional mantido em formato digital. Afortunadamente, os usuários podem utilizar boas práticas de segurança para proteger seu dinheiro ou utilizar provedores de serviço que oferecem bons níveis de seguro contra perda e roubo.

> O problema é a segurança da carteira, uma vez que muitas pessoas não sabem armazenar bens digitais com segurança. Usuários podem ter suas chaves de segurança furtadas por harckers, malwares ou até mesmo por descuido pessoal. Assim é importante saber como armazenar sua carteira com segurança. (Uller, 2014)

Há um risco do fechamento das bolsas de negociação, como aconteceu com a bolsa de Hong Kong GBL em novembro de 2013 que desapareceu com US$4,1 milhões em bitcoins, ou um caso mais recente da bolsa de Mx.Gox no Japão que até o ano de 2014 era a maior negociadora que saiu do ar e desapareceu cerca de US$ 350 milhões.

Como não há fiscalização específica, analistas reforçam a necessidade de seguir orientações financeiras básicas para evitar o risco de a transação com moeda virtual se transformar num pesadelo. (Pessanha, 2014)

Ulrich (2014) observa que os principais problemas de segurança estão associados a “empresas com práticas de gestão ruins e segurança de rede precária e a descuidos dos usuários”.

Muitas carteiras de troca e virtuais sofreram falhas de segurança no passado e a maioria dos serviços ainda não proporcionam segurança necessária para serem utilizados para guardar a moeda como os bancos fazem.

Uma carteira de bitcoin é como uma carteira com dinheiro. Se você não deixaria 1.000 dólares em seu bolso, talvez você deva ter a mesma consideração com a sua carteira de bitcoin. Em geral, é uma boa prática deixar uma quantidade

pequena de bitcoin em seu computador, celular ou servidor para uso diário e deixar o restante dos seus fundos em um ambiente seguro.

Armazenado em um lugar seguro, um backup da sua wallet pode lhe proteger contra falhas humanas e dos computadores. Ele também permitirá que você recupere sua wallet após ter seu celular ou computador roubado, se você mantiver sua wallet encriptada. Criptografar sua carteira ou seu smartphone permite que você defina uma senha para que ninguém tente retirar seus fundos. Isso ajuda a proteger contra os ladrões, porém não pode proteger contra keylogging de hardware ou software.

Uma carteira offline, também conhecida como cold storage (armazenamento frio), provê o mais alto nível de segurança para a sua poupança. Trata-se de armazenar uma carteira em local protegido que não está ligado à rede. Quando feito corretamente, pode oferecer uma boa proteção contra vulnerabilidades de computadores. Usando uma carteira offline em conjunto com backups e criptografia é também uma boa prática.

Utilizar a versão mais recente do software bitcoin permite que você receba correções estáveis e seguras. As atualizações podem prevenir problemas de várias severidades, incluindo novas funcionalidades e mantendo sua carteira segura. Instalar as atualizações para todos os outros softwares do seu computador ou dispositivo móvel também é importante para manter sua carteira em um ambiente seguro.

4 IOTA

A Iota que também é uma moeda digital, fundada por David Sonstebo, tem uma tecnologia diferente das demais moedas. Essa moeda não utiliza de um sistema com blockchain como as demais moedas, dessa maneira solucionando as limitação que a blockchain traz. A Iota vem com uma nova tecnologia chamada de tangle que logo mais falaremos sobre ela.

> Em geral, uma criptomoeda baseada em tangle funciona da seguinte maneira. Em vez de um grande bloco(blockchain), há um DAG- Diagrama Acíclico Direcionado que chamamos de Tangle. (Popov, 2017, p. 2)

Até o momento do desenvolvimento deste trabalho a Iota é a única criptomoeda que não se baseia no sistema de blockchain, que ao contrário da Iota as demais moeda foram desenvolvidas com base no sistema bitcoin a princípio. Essa moeda foi desenvolvida pensando na tecnologia IoT – Internet of Things(Internet das coisas). Internet das coisas seria basicamente a conexão de coisas a internet, como carro, casa, entre outros dispositivos, através de sensores e a programação, de maneira que permita que a coleta de dados e o controle dos mesmos através da internet. Como fala Atzoti, Iera, & Morabito (2010) a internet das coisas é uma presença generalizada de uma variedade de coisas, objetos e sensores.

> Esses objetos, combinados com sistemas automatizados, porem ajudar a coletar informações em tempo real, analisa-las e criar ações de resposta conforme a necessidade. Dessa forma, a Internet das Coisas nada mais é do que uma expansão da conectividade. (Moraes , 2017)

A tecnologia desenvolvida revolucionou a forma de pagamentos, de maneira em que as outras tecnologias desenvolvidas de acordo com a blockchain, já que a seguinte moeda não tem nenhuma taxa a ser paga por transação, pois a mesma possibilita as micro-transferências, coisa que as demais moeda não permitem.

> Especificamente, nos sistemas atualmente disponíveis, você deve pagar uma taxa por fazer uma transação; então, transferir uma quantidade muito pequena não faz sentido desde que teria também que pagar a taxa que é muitas vezes maior. (Popov, 2017, p. 1)

4.1 TANGLE

O tangle é uma tecnologia que segue com intuito de funcionar com a Internet da Coisas, já que a mesma permite transações de pequeno porte, e assim como a bitcoin consegue ser uma tecnologia descentralizada e sem meios para regularizarem por meio de bancos e outras empresas reguladoras, com uma diferença devido a não utilização um sistema de blockchain, e a mesma não cobrar nenhuma taxa. Diferente da blockchain a tangle funciona com uma tecnologia

chamada de DAG – Diagrama Acíclico Direcionado com foi dito mais a cima, dessa maneira não sendo preciso uma grande livro razão para registro.

Popov (2017) nos fala que para realizar uma transação, um nó necessita escolher duas transações para aprovar, verifica se as transações não são conflitantes, e para a validação de uma transação o nó necessita resolver um enigma criptográfico parecido com o que existe na mineração do bitcoin.

A imagem abaixo é uma figura que mostra de forma ilustrativa como funcionada o sistema tangle.

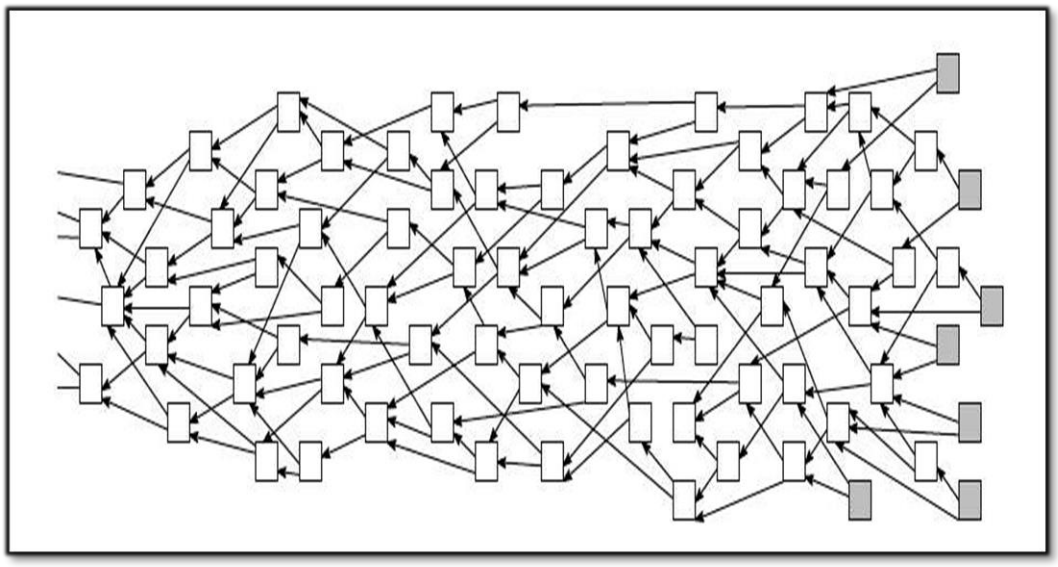

Figura 8 Tangle

Fonte: (Bitcoin Forum, 2015)

O esquema utilizado pelo tangle ao invés de utilizar o sistemas de blocos como é feito no bitcoin o esquema utilizado e parecido com o de árvore que segundo Popov (2017) ele permite a redução de tempo de confirmação, e melhora a segurança geral da rede.

5 METODOLOGIA

O intuito desse estudo foi realizar uma pesquisa, que de acordo com Prodanov & de Freitas (2013) a Pesquisa Científica visa a conhecer cientificamente um ou mais aspectos de determinado assunto.

A execução da pesquisa trouxe um conhecimento parcialmente novo. Assim foi possível falar sobre os bitcoins e as criptomoeda e as relações com as pessoas.

Utilizando de um pesquisa exploratória que segundo Prodanov & de Freitas (2013) visa a proporcionar maior familiaridade com o problema, tornando-o explícito ou construindo hipóteses sobre ele.

Pesquisa foi desenvolvida em cima de uma pesquisa qualitativa afim de encontrar por resultados através de números.

> Como as amostras geralmente são grandes e consideradas representativas da população, os resultados são tomados como se constituíssem um retrato real de toda a população alvo da pesquisa. (Engel & Tolfo, 2008, p. 28)

Na pesquisa realizada foi utilizada um software para a disseminação do questionários e dessa maneira também a geração dos gráficos utilizados nesse estudo. O software utilizado foi desenvolvido pela empresa Google e tem o nome de Google Forms e de acordo com da Silva Kauark, Castro, & Medeiros (2012) O Questionário, numa pesquisa, é um instrumento ou programa de coleta de dados. A confecção é feita pelo pesquisador; o preenchimento é realizado pelo informante.

Dessa forma as informações fundamentais para o desenvolvimento teve partido da pesquisa bibliográfica.

> a pesquisa bibliográfica é aquela que se realiza a partir do registro disponível, decorrente de pesquisas anteriores, em documentos impressos, como livros, artigos, teses etc. Utiliza se de dados ou de categorias teóricas já trabalhados por outros pesquisadores e devidamente registrado. Os textos tornam-se fontes dos temas a serem pesquisados. O pesquisador trabalha a partir das contribuições dos autores dos estudos analíticos constantes dos textos. (Severino, 2010, p. 122)

Os dados coletados foram quantificados de maneira percentual e então apresentados no questionário que foi respondido em sua maioria por pessoas do estado da Paraíba. E para um melhor entendimento foram colados em gráficos.

6 QUESTIONÁRIO SOBRE USO DA MOEDA VIRTUAL

Foi aplicado um questionário com diversas pessoas com ocupações distintas, com o interesse de coletar informações dessas pessoas a respeito dos seus conhecimentos e entendimentos sobre moedas virtuais, mais precisamente sobre a moeda bitcoin, e o que as mesmas tem achado a respeito dessa nova tecnologia que vem crescendo.

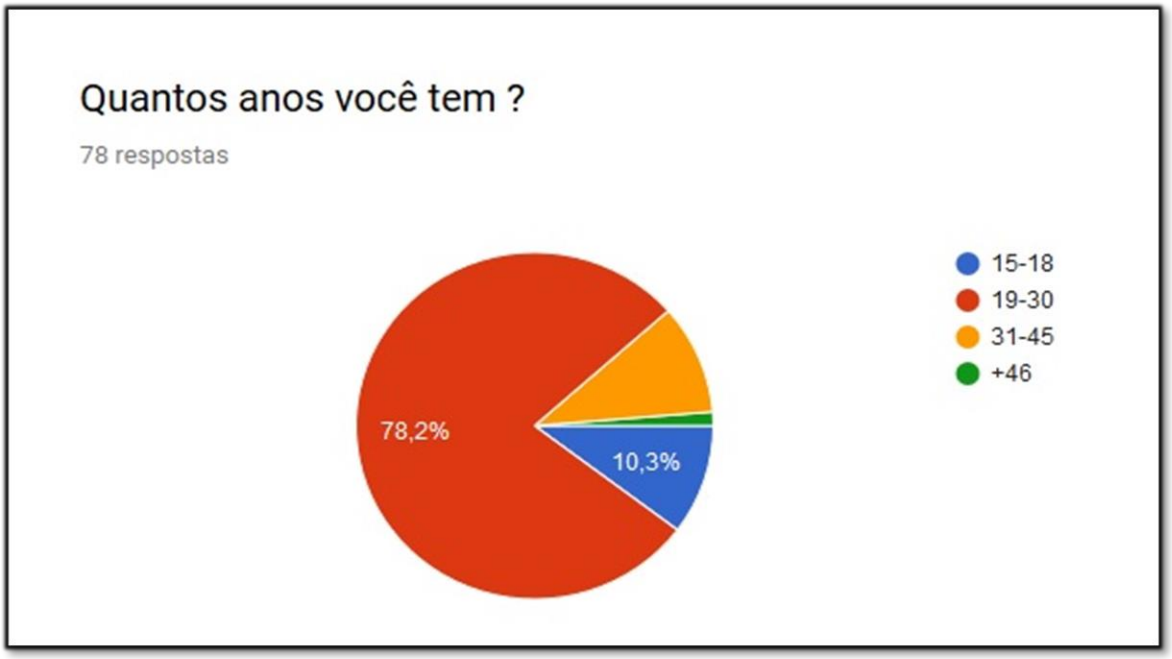

Gráfico 2 - Faixa etária

Fonte: Próprio autor

O gráfico 2 mostrou que a maior parte das pessoas que responderam o questionário foram de uma faixa etária de idade de 19 a 30 anos.

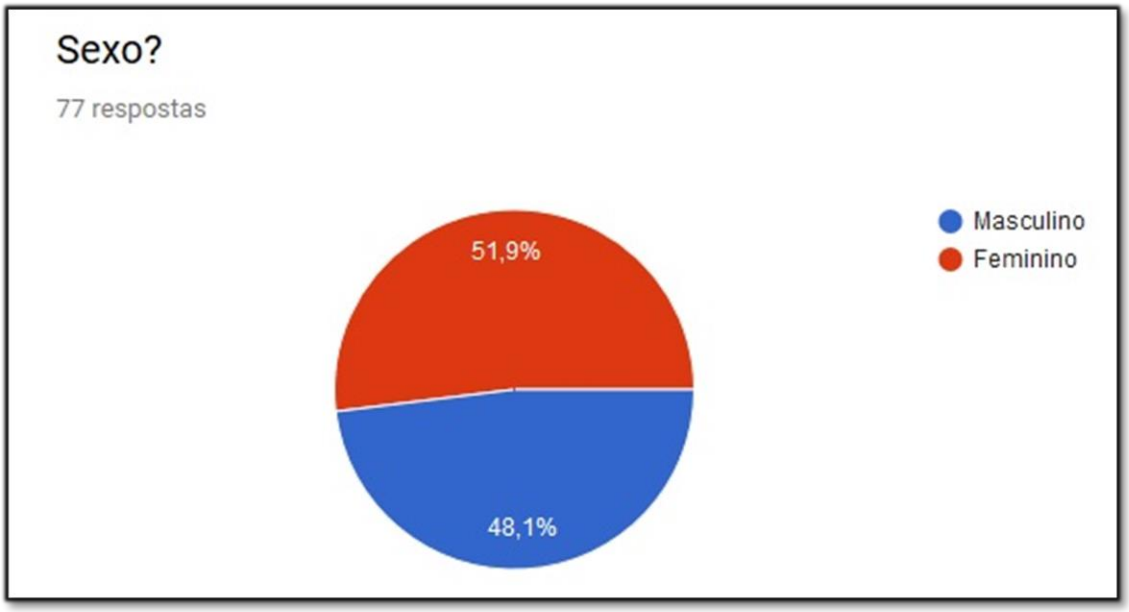

Gráfico 3 - Sexo

Fonte: Próprio autor

Já no gráfico 3 podemos observar que na maioria dos participantes que responderam o questionário são pessoas do sexo feminino.

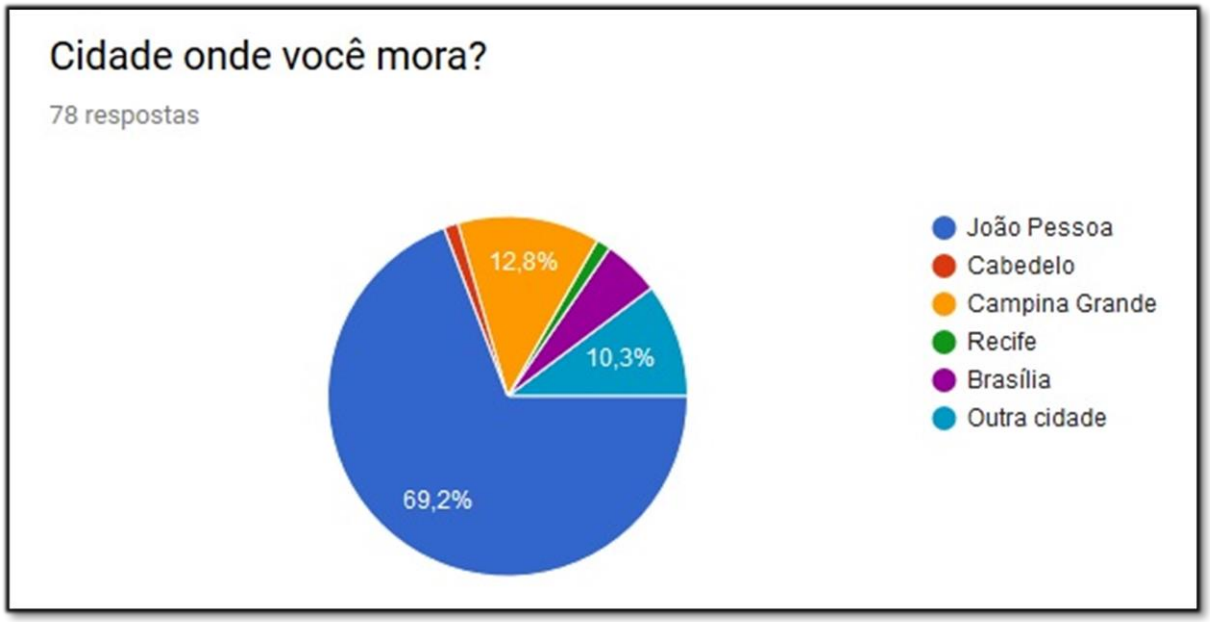

Gráfico 4 - Cidade onde mora

Fonte: Próprio autor

O questionário aplicado atingiu algumas partes dos pais, porém o mesmo teve um maior número de participantes vindo do estado da Paraíba, e que assim podemos ver no gráfico 4, que grande parte dessas pessoas seriam da cidade de João Pessoa.

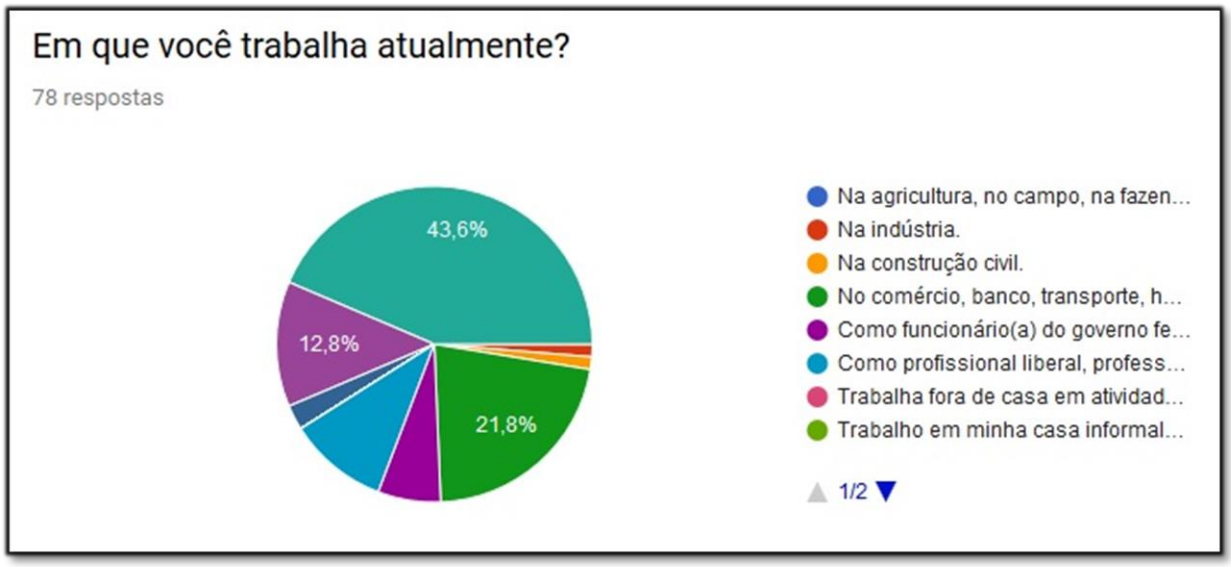

Gráfico 5 - Trabalho atual

Fonte: Próprio autor

Nesse momento da pesquisa, foi aplicada uma questão para determinar quais os setores de atuação dos participantes do questionário, para mostrar que pessoas de setores diferentes contribuíram com os resultados, e podemos ver no gráfico 5 que em sua maioria são pessoas que atual como profissionais liberais, professores e técnicos de nível superior.

Logo em seguida temos pessoas das áreas do comércio, banco, transporte, hotelaria ou outros serviços.

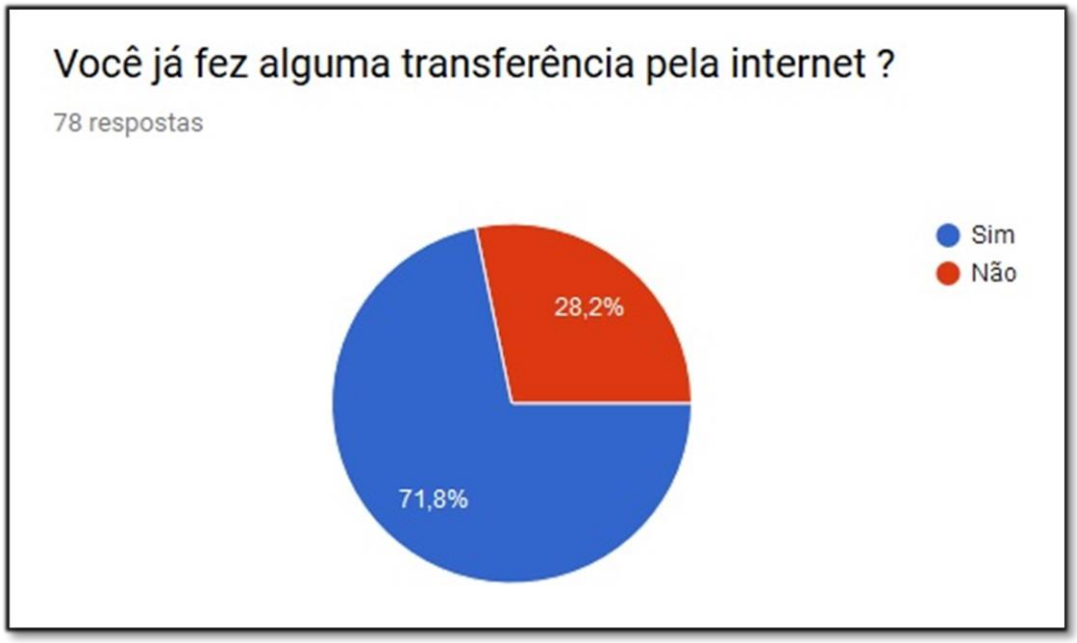

Gráfico 6 - Transferência pela internet

Fonte: Própria autor

A pergunta a respeito do gráfico 6 nos traz uma informação acerca de que as pessoas tem algum conhecimento de transferência através da internet, já que com o crescimento da tecnologia pessoas então utilizando de mecanismos como por exemplo o celular para fazer transferência, a maioria das pessoas responderam que sim, que já fizeram alguma transferência pela internet.

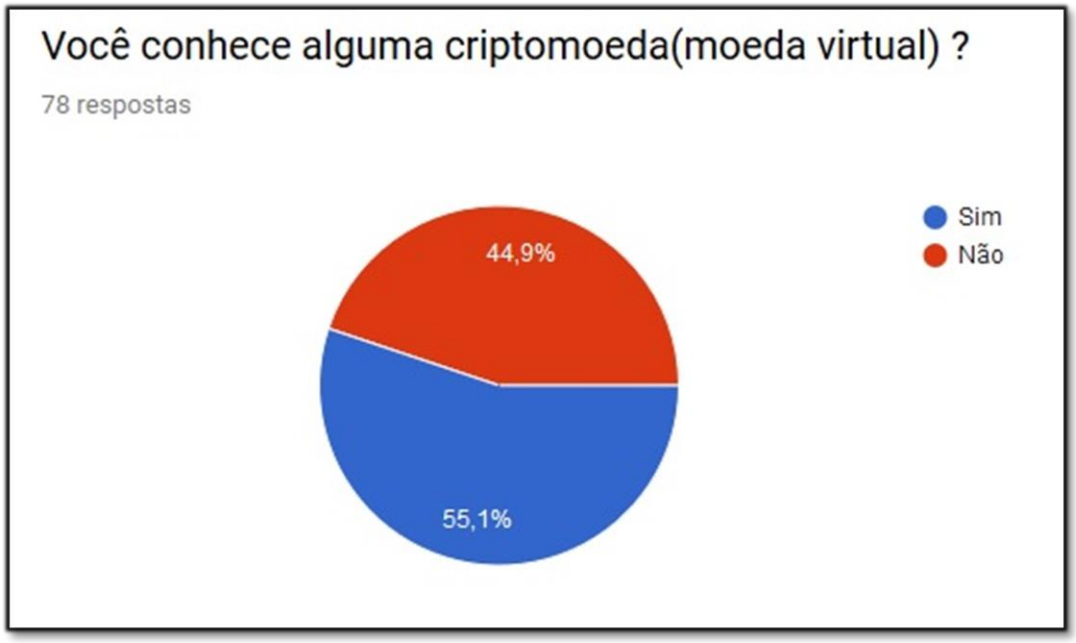

Gráfico 7 - Conhece alguma criptomoeda

Fonte: Próprio autor

O gráfico 7 fala a respeito de conhecer alguma criptomoeda, o gráfico mostra que as moedas virtuais vem de fato tendo uma maior visibilidade e que as pessoas vem tendo um conhecimento por parte delas, já que o mesmo mostra que a maioria das pessoas que participaram informaram que sim, tem algum conhecimento sobre moedas virtuais.

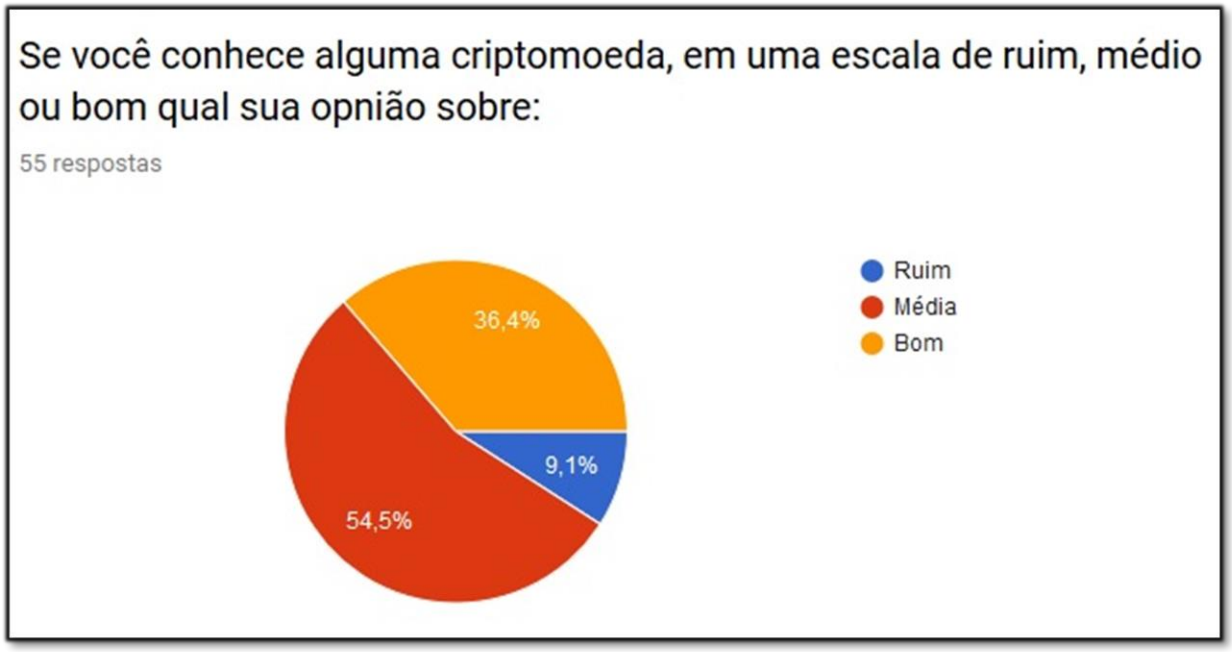

Gráfico 8 - Opinião ruim, média ou boa

Fonte: Próprio autor

Sobre a perspectiva de qualificação, o gráfico 6 aborda uma visão pessoal sobre as criptomoedas em uma escala, de maneira que as mesmas conheçam alguma criptomoeda, e assim a maioria optou pela opção média, seguida da opção boa.

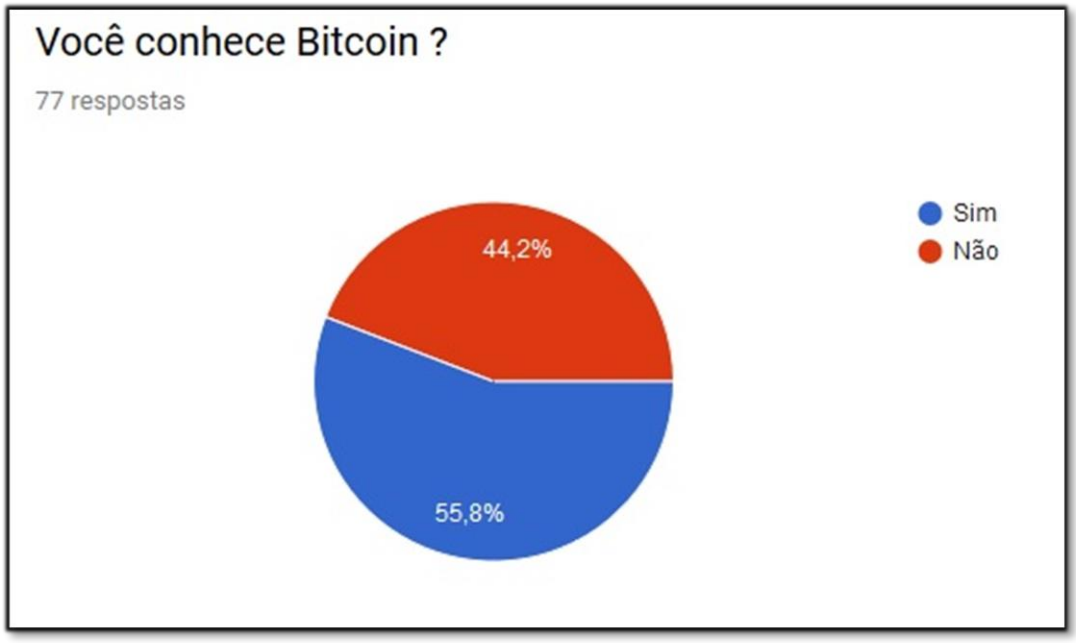

Gráfico 9 - Conhece Bitcoin

Fonte: Próprio autor

Como podemos observar o gráfico 9, que o bitcoin está tendo uma maior visibilidade e que as maioria das pessoas participantes do questionário conhecem a moeda bitcoin.

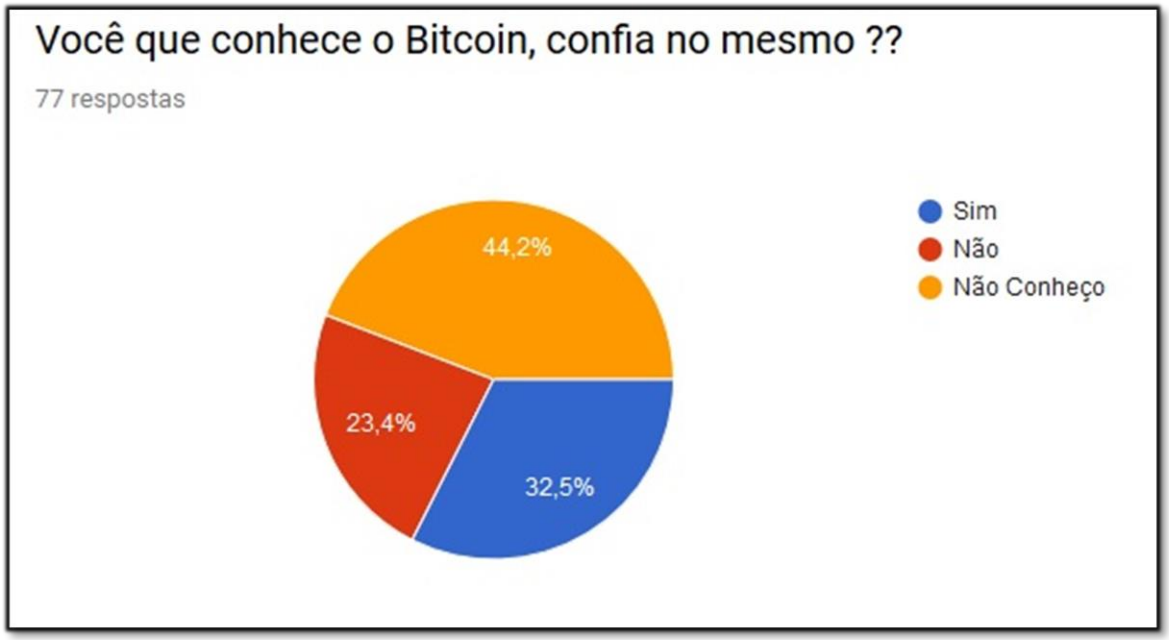

Gráfico 10 - Confia em Bitcoin

Fonte: Próprio autor

Podemos analisar que mesmo com o crescimento do Bitcoin e as moedas virtuais as pessoas ainda tem uma certa insegurança na mesmas, porém vendo o gráfico 10, podemos enxergar que na sua maioria das pessoas que responderam a questão, tem confiança na mesmo.

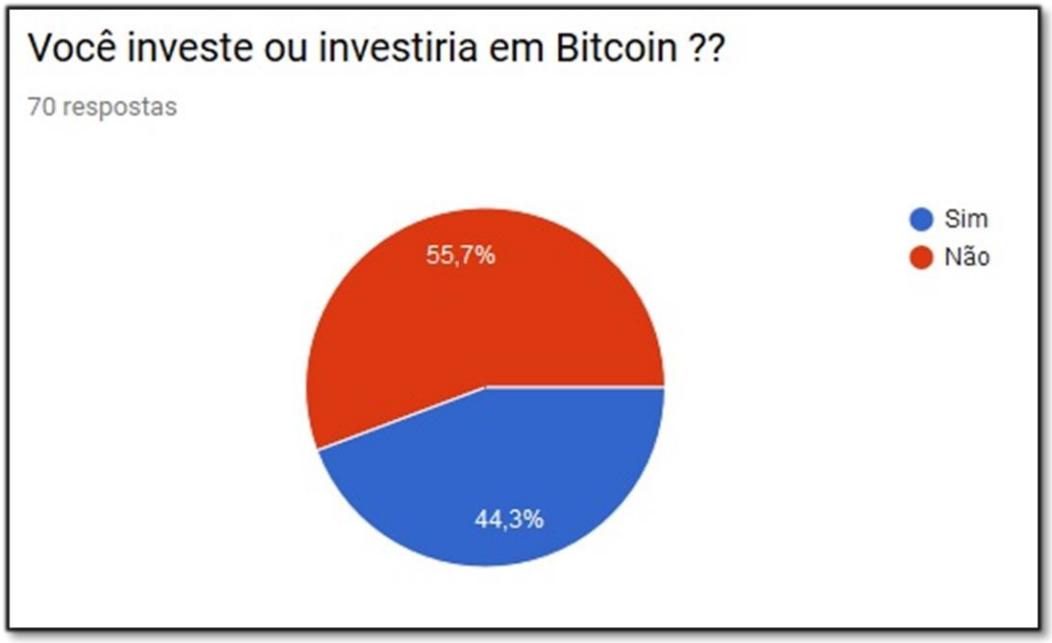

Gráfico 11 - Investimento Bitcoin

Fonte: Próprio autor

Um problema hoje ainda é a falta de conhecimento, e juntamente a ela vem a insegurança, dessa maneira podemos ver que no gráfico 11 as pessoas responderam em maioria não, se elas investem ou fariam investimento na moeda Bitcoin.

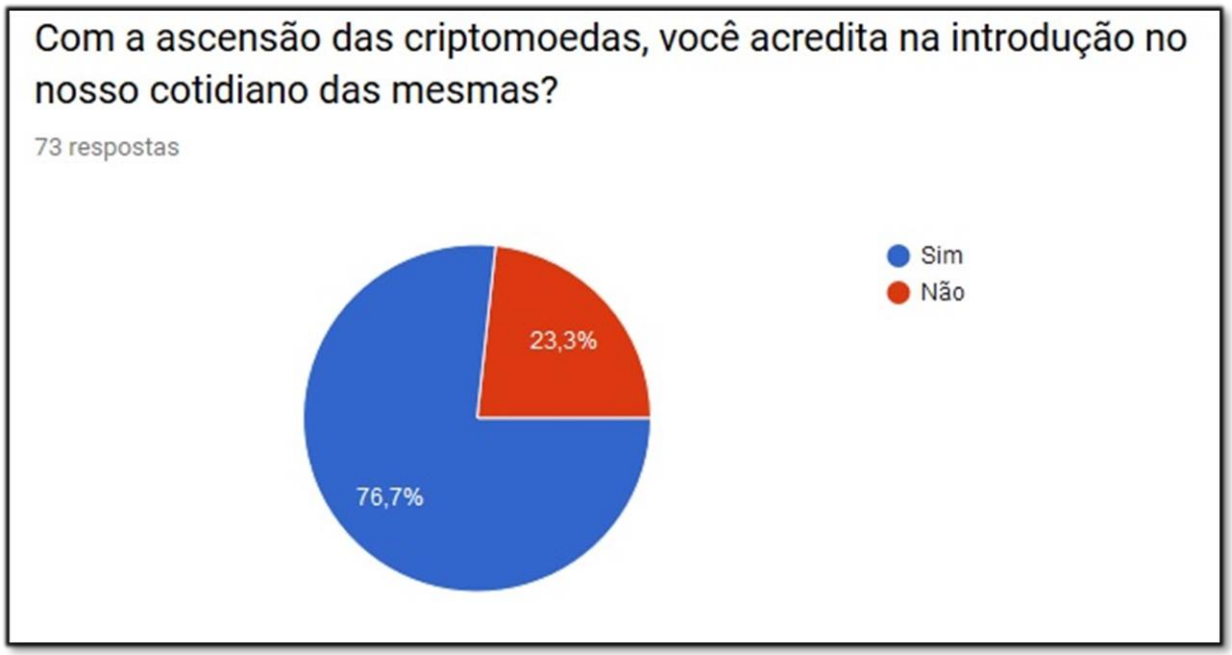

Gráfico 12 - Criptomoedas no cotidiano

Fonte: Próprio autor

Já no gráfico 12 foi abordado a introdução das moedas virtuais no cotidiano das pessoas, de maneira que a pergunta é aborda se as pessoas acreditam que se com a disseminação das moedas elas poderiam fazer parte do dia a dia, sua maioria optou pelo sim, que elas acreditam que essas moedas poderam fazer parte do cotidiano e de certa forma mostrando que existe uma aceitação.

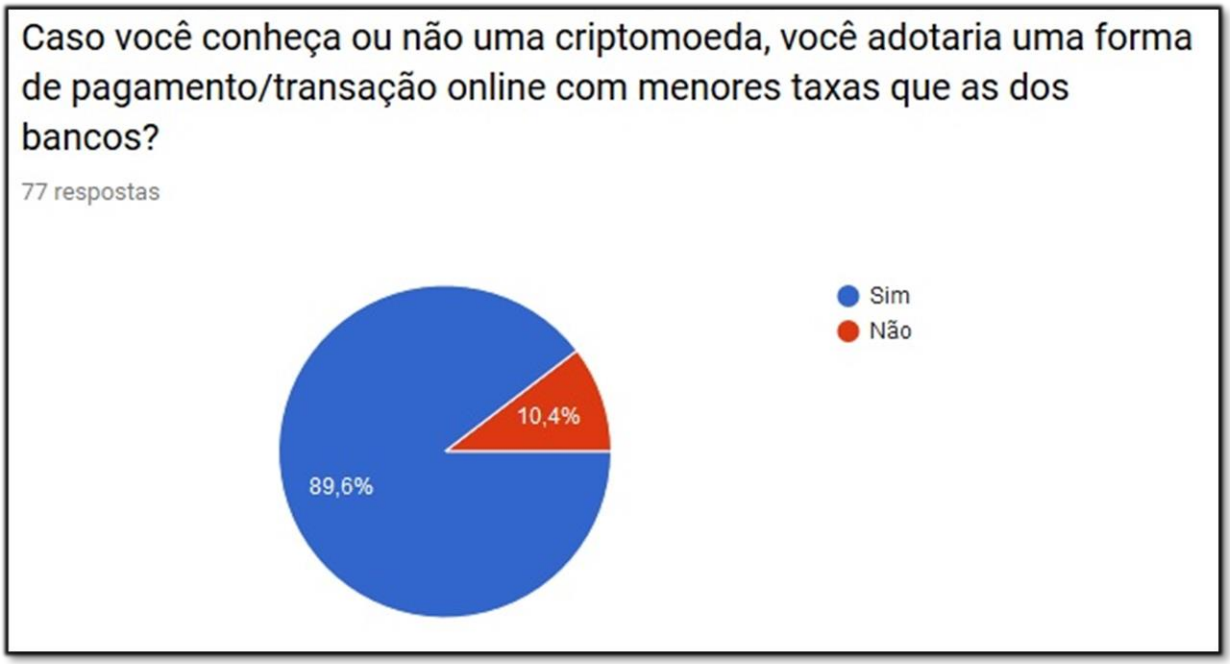

Gráfico 13 - Menores taxas

Fonte: Próprio autor

Em sua maioria nessa questão a cima, podemos analisar o gráfico 13 que a maioria é a favor de uma forma de pagamento e transação online com tarifas de menor preço, de forma que as mesmas não precisem conhecer bitcoin ou outra moeda mas sim a vantagem.

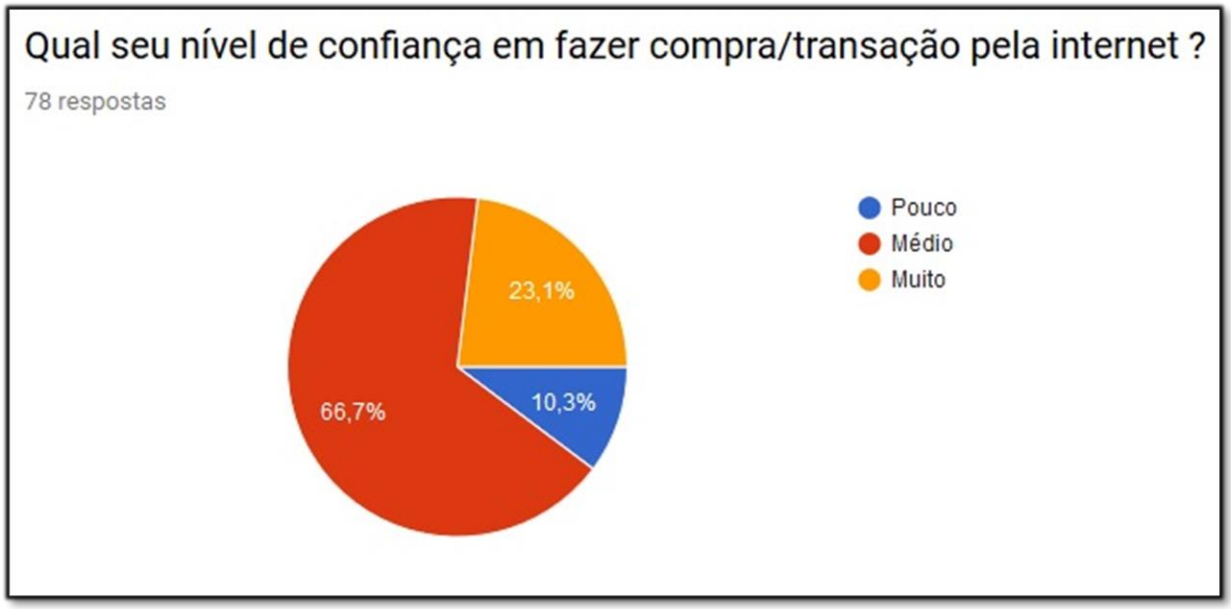

Gráfico 14 - Nível de confiança

Fonte: Próprio autor

Um dos obstáculos ainda é a segurança das pessoas em efetuar pagamentos ou fazer uma transação online pela internet, o gráfico 14 faz uma avaliação das pessoas que participaram respondendo esse questionário num nível de confiança em efetuar esses pagamentos/transações, e sua maioria classificou sua confiança como mediana.

6 CONCLUSÃO

As informações obtidas através da pesquisa para este trabalho possibilitou adquirir conhecimento sobre a importância da tecnologia dos bitcoins e as criptomoedas no dia a dia.

Pode se concluir que o bitcoin é uma moeda assim como os outros papeis moedas, que vem tendo um crescimento exponencial e que as pessoas vem tomando conhecimento sobre a mesma e outras moedas virtuais, assim podendo trazer elas para seu convivo.

Vimos que o sistema funciona com transferências em cima de transmissões criptográfica para manda a integridade das informações transmitidas pela rede.

Uma tecnologia utilizada muito importante é o sistemas de blocos, que é o blockchain, tecnologia ela que faz com que a rede não caia, já que a mesma funciona de forma distribuída, assim um nós sendo derrubado não altera o funcionamento e todos os nós presentes na rede tem uma cópia autentica da blockchain dessa forma evitando fraudes.

Mostramos também que existem vários tipos de carteiras para guardar seus bitcoins, possibilitando a escolha dos usuários de forma que eles possam levar em consideração o nível de segurança e a sua acessibilidade.

A tecnologia dos bitcoin foi criado no ano de 2008 inovando com uma moeda totalmente virtual que não necessita de controladores como bancos e empresas, e que começou valendo praticamente nada e que hoje em dia seu valor subiu consideravelmente.

Essa inovação traz uma outra maneira de pagar contas, transferir dinheiro, com custo mais baixos que os que são impostos pelas instituições financeiras, que prestam esses tipos de serviços.

Vimos que os usuários podem se beneficiar auxiliando na validação das transações se disponibilizando seu poder de processamento, assim sendo bonificado pela rede, assim chama os usuário que fazem isso mineradores.

Apesar de ainda o bitcoin não ser uma moeda de muito conhecimento entre toda a população, e que por falta desse conhecimento pelas mesmas, traz um certo receio, o bitcoin e outras moedas virtuais, vem tendo um crescimento bastante considerável, principalmente pelo fato de cada vez mais a população está se conectando na internet, e assim também fazer cada vez mais transações e compras

onlines já que essa dar uma maior comodidade e muitas vezes melhores preços sobre produtos.

REFERÊNCIAS

ALECRIN, Emerson. **O que é criptografia?**. 11 de agosto de 2009. Fonte: Info Wester. Disponível em: <https://www.infowester.com/criptografia.php>. Acesso em: 12 de outubro de 2017.

ATZORI, Luigi; IERA, Antonio; MORABITO, Giacomo. The Internet of Things: A survey. **Elsevier,** Reggio Calabria, 19, maio, 2010.

BITCOIN. **Bitcoin.org**. Disponível em: <https://bitcoin.org/pt_BR/faq#mineracao>. Acessado em: 15 de outubro de 2017.

BITFINIX. **Bitfinix.** Disponível em: <https://www.bitfinex.com/trading>. Acessado em: 23 de setembro de 2017.

BLOCKCHAIN. **Blockchain.** Disponível em: <https://blockchain.info/wallet/#/home>. Acessado em: 08 de outubro de 2017.

BLOCKCHAIN. **Blockchain paper wallet**. Disponível em: <https://bitcoinpaperwallet.com/>. Acessado em: 14 de agosto de 2017.

BURNETT, Steven; PAINE, Stephen. **Criptografia e Segurança:** O guia oficial do RSA. Rio de Janeiro: Campus, 2002.

COINGATBLOG. **CoinGat Blog. Electrum.** Disponível em: <https://blog.coingate.com/2017/02/setup-electrum-guide/>. Acessado em: 12 de novembro de 2017.

FOXBIT. **Foxbit.** Dispónível em: <https://foxbit.exchange/#trading>. Acessado em: 19 de outubro de 2017.

GERHARDT, Tatiana Engel; SILVEIRA, Denise Tolfo. **Métodos de Pesquisa**: Disciplina DERAD 05. 2008.

IMPERIONANET. **Ganhe seu primeiro Bitcoin**, Conheça tudo sobre a moeda. 2 de janeiro de 2017. Disponível em: <https://imperionanet.com.br/tudo-voce-precisa-saber-minerar-bitcoins/>. Acesso em: 23 de agosto de 2017.

IOTA**.** **Bitcoin Fórum**. 21 de outubro de 2015. Disponível em: <https://bitcointalk.org/index.php?topic=1216479.0>. Acesso: 23 de agosto de 2017.

KAPLANOV, Nikolei. **Nerdy money**: Bitcoin, the private digital currency ,and the case against its regulation. 25 Loy. Consumer L. Rev. 111, 2012

KAUARK, Fabiana da Silva; MANHÃES, Fernanda Castro; MEDEIROS, Carlos Henrique. **Metodologia da Pesquisa:** Um guia prático. Itabuna: Via Litterarum, 2010.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. **Fundamentos de Metodologia Científica.** 5. Ed. São Paulo: Atlas, 2003.

MORAES, Diego. **Você sabe o que é a Internet das coisas e como ela impacta na sua vida?** Fonte: Marketing de Conteúdo. Disponível em: <https://marketingdeconteudo.com/internet-das-coisas/>. Acesso em: 17 de maio de 2017.

NAKAMOTO, Satoshi. **Bitcoin:** A Peer-to-Peer Electronic Cash System. 2008.

PEER-TO-PEER. **O que é Bitcoin e como este dinheiro virtual funciona?** Dicas para computador. Disponível em: <http://www.dicasparacomputador.com/bitcoin-dinheiro-virtual-funciona>. Acessado em: 25 de setembro de 2017.

PESSANHA, Andressa. **Cresce uso do Bitcoin, mas economistas sugerem cautela**. 21 de outubro de 2014. Fonte: PUC-RIO. Disponível em: <http://puc-riodigital.com.puc-rio.br/cgi/CGILua.exe/sys/start.htm?infoid=25231&sid=149#.WicUJSSkpLs>. Acesso em 10 de junho de 2016.

PIGATTO, Daniel. **Segurança em sistemas embarcados críticos - utilização de criptografia para comunicação segura.** ResearchGate. Disponível em: <https://www.researchgate.net/profile/Daniel_Pigatto2/publication/298421681/figure/fig3/AS:340254566436873@1458134418718/Figura-33-Processo-da-criptografia-assimetrica-Adaptado-de-Pires-2010.png>. Acessado em: 12 de novembro de 2017.

PIROPO, Benito. **Bitcoin**: você sabe o que é isto?. 15 de março de 2014. Fonte: Universo BH.. Disponível em: <https://universobh.wordpress.com/2014/03/05/bitcoin-voce-sabe-o-que-e-isto-artigo-completo/> . Acesso em: 10 de junho de 2016.

POPOV, Serguei. **The tangle**. 2017.

REISSWITZ, Flávia. **Análise De Sistema.** Vol. 2. 2008.

SEVERINO, Antônio Joaquim. **Metodologia do Trabalho Científico**. 23. Ed. São Paulo: Cortez, 2007.

SILVA, Douglas Emanuel da (2014). **Coletânea Luso-Brasileira v** – Gestão da Informação, Cooperação em Redes e Competitividade. Porto: Universidade do Porto.

ULLER, Leonardo Pires. **Bitcoin**: saiba como investir e quais os riscos da moeda virtual. 28 de fevereiro de 2014. Fonte: Infomoney. Disponível em: <http://www.infomoney.com.br/onde-investir/acoes/noticia/3183716/bitcoin-saiba-como-investir-quais-sao-riscos-moeda-virtual>. Acesso em: 05 de junho de 2016.

ULRICH, Fernando (2014). **Bitcoin** - A moeda na era digital. São Paulo: Mises Brasil.

ULRICH, Fernando (2015). **Bitcoin ou Blockchain?.** Fonte: InfoMoney. Disponível em: <http://www.infomoney.com.br/blogs/moeda-na-era-digital/post/4020628/bitcoin-blockchain>. Acesso em 14 de abril de 2016.

APÊNDICE

Questionário da pesquisa

Informações gerais

1. Quantos anos você tem?

☐ 15 – 18 anos

☐ 19 – 30 anos

☐ 31 – 45 anos

☐ +45 anos

2. Sexo?

☐ Masculino ☐ Feminino

3. Cidade onde você mora?

☐ João Pessoa

☐ Cabedelo

☐ Campina Grande

☐ Recife

☐ Brasília

☐ Outra Cidade

4. Em que você trabalha atualmente? (Marque apenas uma resposta)

☐ Na agricultura, no campo, na fazenda ou na pesca.

☐ Na agricultura, no campo, na fazenda ou na pesca.

☐ Na construção civil.

☐ No comércio, banco, transporte, hotelaria ou outros serviços.

☐ Como funcionário(a) do governo federal, estadual ou municipal.

☐ Como profissional liberal, professora ou técnica de nível superior.

☐ Trabalho fora de casa em atividades informais (pintor, eletricista, encanador, feirante, ambulante, guardador/a de carros, catador/a de lixo).

☐ Trabalho em minha casa informalmente (costura, aulas particulares, cozinha, artesanato, carpintaria etc.).

☐ Faço trabalho doméstico em casa de outras pessoas (cozinheiro/a, mordomo/governanta, jardineiro, babá, lavadeira, faxineiro/a, acompanhante de idosos/as etc.).

☐ No lar (sem remuneração).

☐ Outro.

☐ Não trabalho.

5. Você já fez alguma transferência pela internet?

☐ Sim ☐ Não

6. Você conhece alguma criptomoeda?

☐ Sim

☐ Não

7. Se você conhece alguma criptomoeda, em uma escala de ruim, médio ou bom qual sua opinião sobre:

☐ Ruim

☐ Médio

☐ Bom

8. Você conhece Bitcoin?

☐ Sim

☐ Não

9. Você que conhece o Bitcoin, você confia no mesmo?

☐ Sim

☐ Não

☐ Não Conheço

10. Você investe ou investiria em Bitcoin?

☐ Sim

☐ Não

11. Com a ascensão das criptomoedas, você acredita na introdução no nosso cotidiano das mesmas?

☐ Sim

☐ Não

12. Caso você conheça ou não uma criptomoeda, você adotaria uma forma de pagamento/transação online com menores taxas que as dos bancos?

☐ Sim

☐ Não

13. Qual seu nível de confiança em fazer compra/transação pela internet?

☐ Sim

☐ Não

14. Você conhece as formas de transações eletrônicas?

☐ Sim

☐ Não