Universidade Federal de Juiz de Fora
Instituto de Ciências Exatas
Programa de Pós-Graduação em Ciência da Computação

Helder Luiz Palmieri Caldas

Estudo da Dinamicidade do Sistema Bitcoin

Juiz de Fora
2016

Helder Luiz Palmieri Caldas

Estudo da Dinamicidade do Sistema Bitcoin

Dissertação apresentada ao Programa de Pós-Graduação em Ciência da Computação da Universidade Federal de Juiz de Fora, na área de concentração em Redes de Computadores, como requisito parcial para obtenção do título de Mestre em Ciência da Computação.

Orientador: Alex Borges Vieira

Juiz de Fora

2016

Ficha catalográfica elaborada através do Modelo Latex do CDC da UFJF
com os dados fornecidos pelo(a) autor(a)

Luiz Palmieri Caldas, Helder.
Estudo da Dinamicidade do Sistema Bitcoin / Helder Luiz Palmieri Caldas. – 2016.
70 f. : il.

Orientador: Alex Borges Vieira
Dissertação (Mestrado) – Universidade Federal de Juiz de Fora, Instituto de Ciências Exatas. Programa de Pós-Graduação em Ciência da Computação, 2016.

1. Bitcoin. 2. P2P. 3. Criptomoedas. 4. *Blockchain*. I. Borges Vieira, Alex, II. Título.

Helder Luiz Palmieri Caldas

Estudo da Dinamicidade do Sistema Bitcoin

Dissertação apresentada ao Programa de Pós-Graduação em Ciência da Computação da Universidade Federal de Juiz de Fora, na área de concentração em Redes de Computadores, como requisito parcial para obtenção do título de Mestre em Ciência da Computação.

Aprovada em: 07 de Março de 2016

BANCA EXAMINADORA

Prof. Dr. Alex Borges Vieira - Orientador
Universidade Federal de Juiz de Fora

Professor Dr. Victor Stroele de Andrade Menezes
Universidade Federal de Juiz de Fora

Professor Dr. Daniel Sadoc Menasche
Universidade Federal do Rio de Janeiro

Dedico essa dissertação a vó Sebastiana Mendes Palmieri(in memoriam), minha força exterior e exemplo.

AGRADECIMENTOS

Agradeço primeiramente aos Deuses por me dar força, coragem e sabedoria para vencer os momentos difíceis.

A toda minha família, em especial aos meus pais e minha avó materna.

A minha namorada Raquel Rezende e meu irmão por todo apoio nos momentos difíceis.

Ao meu orientador e amigo de longa data Alex Borges. Pela paciência, disposição e por acreditar que eu poderia ser capaz de terminar o curso de mestrado. Obrigado sinceramente pela oportunidade e confiança.

Aos amigos que fiz no mestrado, obrigado pela ajuda e incentivo.

Aos amigos e colegas de trabalho do IF Norte de Minas Gerais campis Teófilo Otoni e Almenara e aos amigos do CEFET campus Leopoldina. Obrigado pelo apoio de todos. Vocês sempre me apoiaram e colaboraram com minhas necessidades.

Aos meus professores Marco Antônio Pereira Araújo e Patrícia Lima Quintão que confiaram na minha capacidade de realizar o curso de mestrado.

A todos que de forma direta ou indireta me apoiaram na conclusão do curso.

Meus sinceros agradecimentos a todos! Obrigado!

RESUMO

O Bitcoin é um sistema de pagamento totalmente digital independente de uma entidade centralizadora como bancos ou governos. O projeto foi criado e publicado em 2008 através da Internet. Entretanto apenas em 2009 a rede tornou-se operacional. O Bitcoin é um protocolo de código aberto e uma rede ponto a ponto de participantes que é responsável pelo funcionamento do sistema. Segurança criptográfica, ausência de taxas e de custos de instalação são fatores que convenceram várias empresas do mundo a adotá-lo como alternativa de pagamento. Apesar dos trabalhos acerca da moeda digital, pouco ainda se sabe sobre sua topologia e características, principalmente pela ótica de ciência de redes. Nesse sentido, o presente trabalho apresenta o estudo da dinamicidade de suas principais variáveis no seu funcionamento diário. No decorrer do trabalho são apresentadas duas formas de extração de dados da rede Bitcoin para futuras análises.

Palavras-chave: Bitcoin. P2P. *Blockchain*.

ABSTRACT

Bitcoin is a fully digital payment system independent of a centralized entity like banks or governments. The Bitcoin project was created and published in 2008. In 2009 the Bitcoin P2P network became operational. The Bitcoin is an open source protocol and a peer-to-peer network of participants that is responsible for operating the system. Cryptographic security, absence of exogenous rates and of installation costs convinced several companies in the world to adopt it as a payment alternative. Although, there is an increasing amount of work on digital currencies, little is known about Bitcoin its topology and characteristics, particularly from the viewpoint of network science. In this sense, this paper presents the study of the dynamics of its main variables and their daily functioning. During the work we present two forms of network data extraction Bitcoin for further analysis.

Key-words: Bitcoin. P2P. Blockchain.

LISTA DE ILUSTRAÇÕES

Figura 1 – Representação da Estrutura da Internet [Newman, 2003]. 20
Figura 2 – Representação do Sistema Bitcoin [F. Reid e M. Harrigan, 2011]. . . . 21
Figura 3 – Redes Aleatórias e sua distribuição de grau caracterizando uma distribuição de *Poisson*(normal-Gaussiana) [P. Erdos e A. Rényi, 1959]. . . . 21
Figura 4 – Rede pequeno mundo [Strogatz, 2001] 22
Figura 5 – Rede livre de escala e sua distribuição de graus seguindo a lei da potência [Barabási e Albert, 1997]. 24
Figura 6 – Endereços Bitcoins 26
Figura 7 – Carteiras Web 27
Figura 8 – Carteiras providas por hardware 27
Figura 9 – Carteiras para clientes locais 28
Figura 10 – Carteiras para dispositivos móveis 28
Figura 11 – Exemplo esquemático da ligação dos blocos 29
Figura 12 – Blocos prontos para o *blockchain* 30
Figura 13 – Desenho esquemático do *blockchain* e suas ligações 31
Figura 14 – Mineração no sistema Bitcoin 32
Figura 15 – Client Bitcoin original sincronizando com a rede 37
Figura 16 – Modelo relacional proposto por [Spagnuolo, 2013] 39
Figura 17 – *View* principal proposta por [Spagnuolo, 2013] 39
Figura 18 – Exemplo de busca realizada na base de dados. 40
Figura 19 – Transações Diárias Outubro de 2013 44
Figura 20 – Transações Diárias Novembro de 2013 44
Figura 21 – Diárias Dezembro de 2013 45
Figura 22 – Diárias-Out/Nov/Dez - 2013 45
Figura 23 – Relação Transações Diárias x Volume de bitcoins-Outubro/2013 46
Figura 24 – Relação Transações Diárias x Volume de bitcoins-Novembro/2013 . . . 47
Figura 25 – Relação Transações Diárias x Volume de bitcoins-Dezembro/2013 . . . 47
Figura 26 – Volume Diário de bitcoin Transacionando-Out/Nov/Dez-2013 48
Figura 27 – Endereços Únicos Usados no Sistema Bitcoin-Out/Nov/Dez-2013 . . . 49
Figura 28 – Comparação Volume Transacionado x Endereços Únicos-Nov/2013. . . 50
Figura 29 – Comparação entre Volume Transacionado x Endereços Únicos-Out/2013. 50
Figura 30 – Comparação entre Volume Transacionado x Endereços Únicos-Dez/2013. 51
Figura 31 – Informação dos Blocos no Sistema Bitcoin [Spagnuolo, 2013] 52
Figura 32 – Tempo de Confirmação dos Blocos 52
Figura 33 – Cotação da moeda bitcoin(fonte: http://www.coindesk.com/price/) . . 53
Figura 34 – Comparação Cotação x Volume de Bitcoins 54
Figura 35 – Curva de Crescimento baseado no número de transações. 55
Figura 36 – Curva de Crescimento baseado no número de Usuários. 56

Figura 37 – Crescimento do Blockchain 57
Figura 38 – Grau dos 25 nós mais importantes no mês de Novembro/2013 60
Figura 39 – Grau dos 25 nós mais importantes no mês de Fevereiro/2014 61
Figura 40 – Identificando usuários 1. 62
Figura 41 – Identificando usuários 2. 62
Figura 42 – Identificando usuários 3. 63
Figura 43 – Identificando usuários 4. 63
Figura 44 – Distribuição de Grau-Novembro/2013 64
Figura 45 – Distribuição de Grau-Fevereiro/2014 65

LISTA DE TABELAS

Tabela 1 – Total de Transações dos meses de Novembro 43
Tabela 2 – Número de transações mês antes e após o fechamento do *Silk Road* . . 43
Tabela 3 – Volume Total de bitcoins Transacionados Mês. 46
Tabela 4 – Endereços Bitcoins únicos. 49
Tabela 5 – Número de Nós analisados nos dois períodos 59
Tabela 6 – Número de Nós sem Grau nos dois períodos 59
Tabela 7 – Número de Nós Com Grau 1 60

LISTA DE ABREVIATURAS E SIGLAS

DHT Distributed Hash Tables

ECDSA Elliptic Curve Digital Signature Algorithm

P2P Peer-to-Peer

SUMÁRIO

1 Introdução 13
1.1 Objetivos 14
1.2 Organização da Dissertação 14

2 Conceitos Teóricos 16
2.1 Características Básicas de Redes P2P 16
2.1.1 Classificação de redes P2P 17
2.1.2 Redes Estruturadas 17
2.1.3 Redes Não estruturadas 17
2.1.4 Classificação das redes não estruturadas 18
2.2 Redes Complexas 19
2.2.1 Conceitos Básicos de Redes complexas 19
2.2.2 Tipos de redes complexas 20

3 Sistema Bitcoin e suas características 25
3.1 Sistema Bitcoin 25
3.2 Funcionamento do sistema Bitcoin 25
3.2.1 Endereço Bitcoin 25
3.2.2 Carteiras Bitcoin 26
3.2.3 Blocos 28
3.2.4 Blockchain 29
3.2.5 Mineração 31
3.2.6 Transações 32

4 Trabalhos Relacionados 34

5 Metodologia e Modelagem 37
5.1 Extração dos dados do Sistema Bitcoin 37
5.2 Realizando Parsing no Blockchain 38
5.2.1 Extraindo dados para análise da estrutura do sistema Bitcoin 40

6 Análise da Dinamicidade do Sistema Bitcoin 42
6.1 Análise das Variáveis Diárias do Sistema Bitcoin. 42
6.2 Volumes Transacionados Diariamente 44
6.3 Usuários participantes no Sistema Bitcoin 48
6.4 Tempo de Confirmação de Blocos 51
6.5 Valor de Negociação do Bitcoin 53

6.6 Crescimento do Sistema Bitcoin 55

7 Caracterização da Topologia da Rede Bitcoin 58
7.1 Identificação de Usuários e Hubs no Sistema Bitcoin 58
7.2 Métrica de Grau para descobrir hubs e usuários importantes. 59
7.3 Identificando usuários 61
7.4 Caracterização da Estrutura da Rede Baseada na Distribuição de Grau. 64

8 Considerações Finais 66

REFERÊNCIAS 67

1 Introdução

O Bitcoin é um sistema de pagamento eletrônico descentralizado que utiliza a rede P2P para sustentar seu funcionamento. É um sistema de código aberto que vem sendo aperfeiçoado desde sua criação. O projeto foi criado e publicado em 2008 através da Internet e com o pseudônimo do criador de Satoshi Nakamoto [Nakamoto, 2008], entretanto apenas em 2009 a rede tornou-se operacional e exatamente no dia 03 de Janiero de 2009 ocorreu o primeiro registro de bitcoin transacionado e registrado pela rede P2P do sistema Bitcoin. Apesar do Bitcoin ser um novo modelo de sistema de pagamento descentralizado e totalmente digital ele não é uma ideia nova. Essa ideia surgiu bem antes, no ano de 1993 baseado no Manifesto *Cypherpunk*, um texto de autoria do programador Eric Hughes que defendia o uso de sistemas baseados em criptografia para proteger a privacidade na era da informação.

Paralelamente ao Bitcoin existem outros sistemas com a mesma ideologia, mas que atualmente não possuem a notoriedade do Bitcoin. O Bitcoin tornou-se consagrado porque foi o primeiro sistema de criptomoedas realmente funcional. Um exemplo de outra criptomoeda é o Litecoin. Mas atualmente existem inúmeros outros modelos de criptomoedas. A invenção do sistema Bitcoin se torna revolucionária porque pela primeira vez o problema do gasto duplo pode ser resolvido sem existir uma terceira entidade centralizadora envolvida no processo.

Após a grande utilização do sistema Bitcoin o mesmo ganhou uma forte atenção da mídia através de jornais importantes como o The Guardian, [Alex Hern, 2013] e a Forbes, [Kashimir Hill, 2013]. A atenção foi motivada pela conversão de valores bitcoins em valores de dólares. Desse modo tornando o sistema Bitcoin não só apenas em um sistema de pagamento descentralizado e sim uma moeda virtual que não deriva de nenhuma moeda real.

Assim, o bitcoin tem seu valor monetário definido através de um mercado aberto da mesma forma que são estabelecidas as taxas de câmbio entre diferentes moedas mundiais. O sistema usa segurança criptográfica para realizar as transações entre os usuários, taxa de transação insignificante, custo de manutenção e instalação zero, e o risco de transações serem desfeitas é minimo após terem sido confirmadas pela rede. Essas características convenceram várias empresas a adota-lo como um novo método de pagamento.

Esse trabalho apresenta a dinamicidade das variáveis do sistema Bitcoin. A dinamicidade é apresentada através da caracterização de suas principais variáveis dinâmicas em seu funcionamento diário. A importância da caracterização das variáveis está ligada

diretamente ao estudo do funcionamento do sistema. Como exemplo o trabalho mostra a variação de transações diárias em comparação a eventos ocorridos fora do sistema Bitcoin. Também com a caracterização das variáveis é possível determinar a tendência do volume de bitcoins transacionados em determinado período. Através da caracterização das variáveis dinâmicas conseguimos apresentar uma tendência de funcionamento do sistema bitcoin. Desse modo o trabalho apresenta formas de retirar informações do *blockchain* e possibilitar o estudo dessas variáveis através de sua caracterização.

A tendência do funcionamento do sistema Bitcoin ocorre de forma bastante dinâmica e suas alterações ocorrem de acordo com cada variável do sistema em específico. O trabalho também apresenta um forma de identificar usuários participantes do sistema Bitcoin. E, por fim, o trabalho mostra qual o modelo de estrutura que a rede do sistema Bitcon segue de acordo com as redes complexas. O trabalho caracteriza que o sistema Bitcoin tem a tendência de estrutura seguindo as redes livres de escala.

1.1 Objetivos

O objetivo do trabalho é apresentar o novo paradigma de criptmoedas que vem sendo inserido no cotidiano mundial através do seu mais forte representante que é o sistema Bitcoin. Este trabalho mostra como retirar informações da rede P2P Bitcoin e, através desses dados, caracterizar a rede para demonstrar seu potencial e seu funcionamento.

- Caracterizar, através da modelagem da base de dados, variáveis dinâmicas pertinentes ao funcionamento diário do sistema Bitcoin.

- Analisar e comparar informações extraídas da base de dados modelada com eventos exteriores ao sistema Bitcoin.

- Identificar importantes nós da rede que possuem grandes volumes de conexão.

- Aplicar métricas de redes complexas para caracterizar a estrutura da rede.

1.2 Organização da Dissertação

A dissertação está organizada da seguinte forma: o capítulo 2 apresenta os conceitos teóricos para o entendimento do sistema Bitcoin, redes P2P e uma breve introdução a redes complexas. No capítulo 3 apresentamos as principais características e definições do sistema Bitcoin. No capítulo 4 apresentamos os trabalhos relacionados ao tema e suas

áreas de atuação no estudo do sistema Bitcoin. O capítulo 5 apresenta a metodologia de captação e extração dos dados para a construção dos gráficos e análises futuras. No capítulo 6 apresentamos os resultados extraídos dos dados coletados e a caracterização das variáveis dinâmicas ao funcionamento do sistema diário. O capítulo 7 aplicamos métricas de redes complexas e apresentamos as características da estrutura da rede. As conclusões e trabalhos futuros são apresentados no capítulo 8.

2 Conceitos Teóricos

Este capítulo apresenta os principais conceitos para o entendimento do funcionamento do sistema Bitcoin, conceitos sobre redes P2P e uma breve introdução a redes complexas.

2.1 Características Básicas de Redes P2P

A definição de redes P2P, de acordo com [Adroutsellis-Theotokis, 2004] é que redes P2P são sistemas distribuídos através de nós interconectados, que podem se reorganizar automaticamente em topologias de rede, com a capacidade de compartilhar recursos. Também apresentam a capacidade de adaptação a falhas e aumento da disponibilidade de nós garantindo escalabilidade que ao mesmo tempo garante conectividade e desempenho, sem a necessidade de servidores centralizados.

- Baixo custo: A rede P2P por ser uma rede distribuída tem seus custos divididos entre seus participantes. Cada participante ajuda a estrutura da rede P2P com seu recurso disponível naquele momento em seu nó.

- Robustez: Redes P2P distribuídas não concentram um único ponto de falha. Comparando com um sistema cliente servidor se ocorrer a indisponibilidade de um único servidor na sua rede ocorre o risco do sistema ficar parado, até que o servidor seja restabelecido. Já na rede P2P um outro nó da rede poderá disponibilizar o serviço até que o ponto falho seja recuperado.

- Flexibilidade: Por ser uma rede descentralizada é possível realizar configurações automáticas e ou configuração dinâmica. Um exemplo de configuração dinâmica ocorre quando um novo nó ingressa na rede e automaticamente recebe as informações pertinentes a rede P2P. Outra característica da flexibilidade é que a qualquer momento os nós podem entrar e sair da rede sem atrapalhar o funcionamento daquele serviço.

- Escalabilidade: Como a rede não possui um servidor central como no modelo cliente x servidor, pode não existir gargalos dependentes de um único ponto. Entretanto, gargalos ainda podem acontecer dependendo da atividade que a rede P2P desenvolve e sua capacidade de atuação no momento. Nas redes P2P o conceito de escalabilidade é facilmente entendido. Quanto maior a quantidade de nós participantes maior é a capacidade de poder computacional e recursos oferecidos pela rede.

O sistema Bitcoin tira proveito das características destacadas por [Adroutsellis-Theotokis, 2004] para se tornar uma rede robusta utilizando uma forte estrutura tecnológica baseada nos conceitos de redes P2P. Outro grande atrativo das redes P2P são seus conceitos de baixo custo, robustez, flexibilidade e escalabilidade.

As redes P2P já são bem conhecidas e definidas. Suas vantagens impulsionam até hoje diversos sistemas em redes de computadores que utilizam seus recursos para seu bom funcionamento. O sistema Bitcoin aproveita dessa forte estrutura e recursos para ser uma tecnologia altamente robusta e promissora. Desse modo podemos compreender um pouco do funcionamento das redes P2P, suas vantagens e quais seus grandes benefícios. Na próxima seção vamos ver como as redes P2P são divididas de acordo com sua estrutura.

2.1.1 Classificação de redes P2P

Basicamente as redes P2P são divididas em dois grupos de classificação. As redes estruturadas e as redes não estruturadas. Essa categorização de redes estruturadas ou não estruturadas é baseada em como os enlaces são formados.

2.1.2 Redes Estruturadas

Redes P2P estruturadas são redes de computadores capazes de fazer o trabalho de que cada nó possa repassar a informação de forma adequada para qualquer nó existente na rede. Entretanto para que os nós façam essa tarefa de forma adequada é necessário que eles se organizem de acordo com critérios e algoritmos específicos. As redes P2P estruturadas utilizam tabelas *hash* distribuídas(DHT).

O DHT(*Distributed Hash Table*) é uma tabela hash tradicional, que associa a identificação ou valores dos nós da rede em uma chave única. A diferença é que a tabela é distribuída entre os nós da rede ficando cada nó responsável por uma parte da tabela *hash*. [Balakrishnan, 2003] DHTs são usadas para tornar as buscas na rede P2P mais eficientes do que nos sistemas não-estruturados.

Alguns sistemas de redes P2P que são estruturados podem ser visualizados em Chord [Stoica, 2001], Pastry [Rowstron, 2001], Tapestry [Stribling, 2004] e CAN [Ratnasamy, 2001].

2.1.3 Redes Não estruturadas

Redes P2P não estruturadas são mais simples por não usarem algoritmos especiais para organizar suas conexões de rede. Assim toda vez que um nó entra na rede é necessário apenas sua atualização com as novas informações da rede P2P. Essas informações são

repassadas ao nó através de seus vizinhos. Após feita essa cópia de informações iniciais o nó já esta apto a criar suas próprias conexões na rede ao longo do tempo.

Algumas redes não estruturadas utilizam a técnica de *flooding* para difundir suas informações pela rede. Entretanto existem redes não estruturadas que utilizam outras técnicas para realizar a sua difusão de informações por toda a rede. A técnica de *flooding* consiste em que um nó envie uma mensagem para todos os outros nós participantes da rede solicitando o recurso necessário ou informando alguma atualização de sua estrutura. Essa metodologia de busca de informações e atualização de informações nas redes P2P não estruturadas causavam uma grande desvantagem em relação as redes estruturadas, pois inundavam a rede com um grande volume de mensagens de controle, assim causando, em determinados momentos, altos picos de tráfego de controle. De acordo com [Adroutsellis-Theotokis, 2004] a rede não estruturada é pouco escalável. Essas redes são divididas em modelos distintos como redes P2P puras, centralizadas ou híbridas conforme descrito a seguir.

2.1.4 Classificação das redes não estruturadas

P2P Pura ou descentralizada: A rede P2P pura é uma rede P2P em que todos os nós da rede são iguais não existe um nó central, assim a rede é completamente descentralizada. Geralmente o sistema de busca e atualização é realizado através do *flooding* que repassa todas as informações a todos os nós da rede. Os nós são responsáveis por manter localmente informações próprias como arquivos de índices e outras informações.

P2P híbrida: No modelo de rede híbrida alguns nós são denominados de super nós que tem como premissa fornecer uma infraestrutura básica. Os super nós funcionam como pequenos servidores centrais [Rocha, 2005]. Os super nós são nós da rede com grandes recursos disponíveis, como poder de processamento, tabelas de informações, arquivos de índices e etc. Os super nós também são os responsáveis por fazer o gerenciamento das buscas na rede, assim como controlar a entrada de novos nós na rede P2P.

P2P centralizada: Nesse modelo de rede um nó central que funciona como um servidor da rede. O servidor central da rede controla as entradas e saídas dos nós da rede. Com essa função de servidor central, todos os nós que se registram na rede, também informam ao servidor central quais os recursos que irão compartilhar na rede. Assim o servidor central sabe exatamente o que todos os nós têm para compartilhar na rede. Entretanto o servidor central apenas possui as informações de onde estão os recursos disponíveis. Já o acesso aos recursos é feito diretamente entre os nós participantes da rede. Um grande problema desse modelo é que a rede apresenta uma grande vulnerabilidade

por possuir um ponto único de falha. Caso esse nó central apresente alguma falha toda a informação de recursos é perdida.

2.2 Redes Complexas

Nessa seção do trabalho são apresentados conceitos básicos de redes complexas, para o bom entendimento do sistema Bitcoin. Esses conceitos explicam em qual cenário o sistema se baseia, seguindo a lógica das redes complexas.

2.2.1 Conceitos Básicos de Redes complexas

Redes complexas são grafos que modelam estruturas lógicas ou físicas não triviais, compostas por vértices (nós) interligados por meio de arestas, conexões [Barabási, 2003]. Através das redes complexas é possível modelar diversos sistemas a fim de resolver problemas específicos. É possível modelar grandes sistemas físicos como, por exemplo, a grande rede de computadores a Internet.

[Newman, 2003] estuda a modelagem da grande rede de computadores que compõe a Internet. Essa modelagem é feita através de grafos, onde temos que os computadores conectados à Internet referem-se aos vértices da rede enquanto que os cabos e meios de transmissão representam as arestas do grafo [Jean Metz, 2007]. Fazendo uma comparação com o sistema Bitcoin podemos fazer uma modelagem parecida com a Internet, onde os nós(usuários) referem-se aos vértices da rede e as transações(tráfego de bitcoins entre os usuários) representam as arestas do grafo. Como ilustração da modelagem de redes complexas como grafos, temos as figuras 1 e 2. A figura 1 mostra a modelagem da Internet de acordo com [Newman, 2003], e a figura 2 mostra a modelagem de um período específico no sistema Bitcoin [F. Reid e M. Harrigan, 2011]. As figuras apresentam como as redes complexas podem modelar grandes sistemas através de grafos. Nas duas figuras podemos visualizar a estrutura de nós e arestas, onde nós são os participantes do sistema modelado e as arestas são responsáveis por realizar a ligação entre os nós.

Um grafo pode ser definido quando um conjunto de vértices e um conjunto de arestas realizam a conexão entre esses vértices. As arestas estabelecem algum tipo de relação entre dois vértices de acordo com o problema modelado. No sistema Bitcoin essa relação representa a transação entre dois usuários integrantes da rede. Toda transação tem um valor que é o montante transferido de um usuário para outro. Os grafos que representam as redes complexas podem ser direcionados ou não. Em um grafo direcionado, cada aresta tem um sentido que é sua direção em que conecta a um vértice origem a um vértice destino. Os grafos direcionados digrafos podem ser cíclicos, quando há um caminho de um vértice para ele mesmo, ou acíclicos quando não existe esse caminho. É importante lembrar que nem todo grafo pode ser considerado uma rede complexa, pois

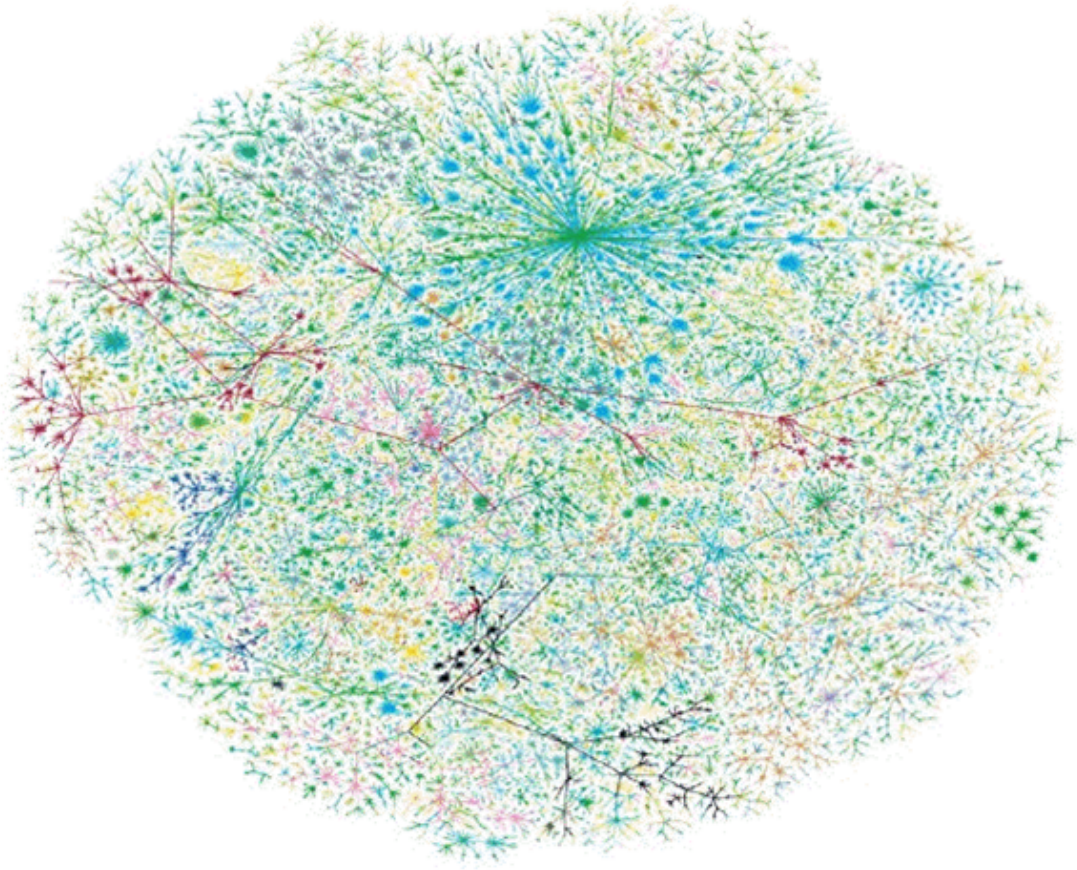

Figura 1 – Representação da Estrutura da Internet [Newman, 2003].

essa classificação só é possível se o grafo apresentar algumas propriedades topográficas que não estão presentes em grafos simples.

2.2.2 Tipos de redes complexas

Nessa seção vamos apresentar os 3 principais modelos de redes complexas: redes aleatórias, redes pequeno-mundo, e redes livre de escala.

Redes aleatórias: proposto por [P. Erdos e A. Rényi, 1959] as redes aleatórias são as redes complexas mais simples. As redes aleatórias são criadas através da ligação aleatória entre os vértices de um conjunto. Essa ligação ocorre de forma que qualquer vértice pode se ligar a outro vértice com probabilidade igual e que todos eles tenham a chance de se conectar a outro elemento da rede.

Acredita-se que o processo de construção da rede seja aleatório no sentido de que vértices se conectam aleatoriamente. Assim todos os vértices de uma determinada rede aleatória têm aproximadamente a mesma quantidade de conexões e as mesmas chances de receberem novas ligações [Barabasi e Albert, 1999]. Uma característica importante

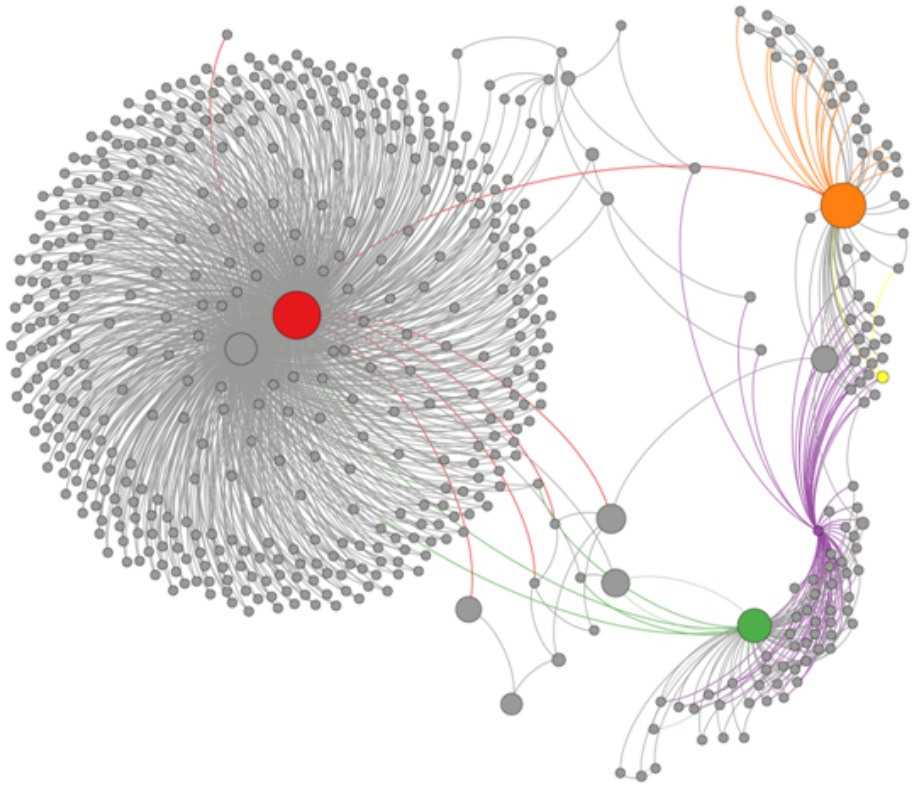

Figura 2 – Representação do Sistema Bitcoin [F. Reid e M. Harrigan, 2011].

das redes aleatórias é que elas apresentam uma distribuição de graus característica: a Distribuição de *Poisson* (normal-Gaussiana) como na figura 3

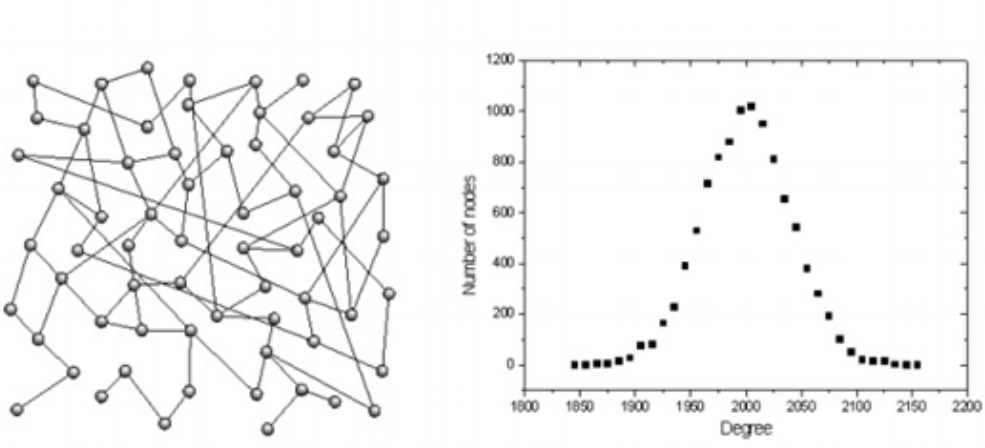

Figura 3 – Redes Aleatórias e sua distribuição de grau caracterizando uma distribuição de *Poisson*(normal-Gaussiana) [P. Erdos e A. Rényi, 1959].

Redes pequeno mundo: Segundo [Watts e Strogatz, 1998], as redes de pequeno mundo apresentam padrões com alto grau de conectividade, que formam pequenas quantidades de conexões nos vértices. Esse modelo proposto é altamente semelhante ao modelo proposto por [P.Erdos e A. Rényi, 1959], onde muitas conexões são criadas entre vértices

mais próximos, apresentando-se como um mundo pequeno. Nesse modelo, a distância média entre dois vértices de uma rede muito grande não ultrapassa um número pequeno de vértices. Para isso, basta que algumas conexões aleatórias entre grupos sejam estabelecidas [Buchanan, 2002].

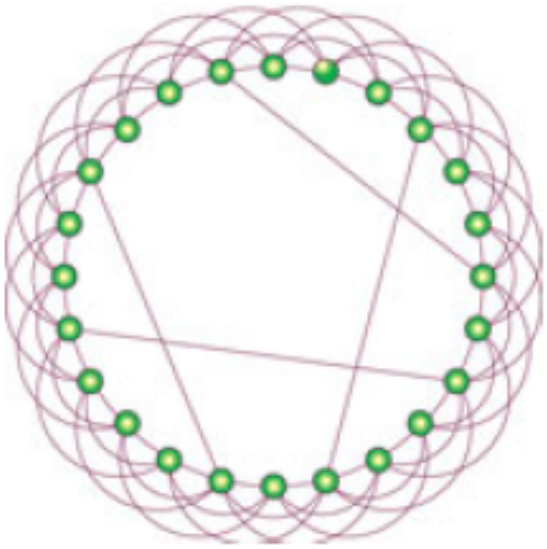

Figura 4 – Rede pequeno mundo [Strogatz, 2001]

A característica de pequeno mundo é observada quando a maioria dos vértices se conecta a outros vértices através do caminho mínimo. O caminho mínimo também é chamado caminho geodésico ou distância geodésica. O caminho mínimo é formado pelo menor caminho que conecte dois vértices usando o menor número de arestas possíveis.

Em 1960 Stanley Milgran, [Stanley Milgran, 1960] realizou um famoso experimento que se uma carta fosse entregue a indivíduos de origem que são aleatoriamente escolhidos e que não fosse o destinatário e essa carta repassada a outro indivíduo assim por diante até chegar o número de 6 passagens ela chegaria ao destinatário. Ao término do experimento os resultados mostravam que as cartas demoravam em média de 5 a 6 passagens até chegar ao seu destinatário. Através desse experimento surgiu o conceito dos seis graus de separação que comprova que pessoas aparentemente sem relação alguma têm uma grande probabilidade de possuírem, em algum grau, amigos em comum que as aproximem.

A teoria proposta por [Stanley Milgran, 1960], foi reproduzida pelo site `www.facebook.com` no ano de 2011 afim de checar o resultado da teoria dos seis graus. A rede social mediu qual a distância que cada um de seus usuários estão distantes entre si. O site

`www.facebook.com` utilizou a seguinte conta. O site apurou o número de amigos de um único usuário e, logo depois quantos amigos únicos(sem repetição) estes amigos possuíam, e assim sucessivamente, até alcançar todos os membros da rede social. O resultado desse experimento que foi realizado com uma população de aproximadamente 1.6 bilhões de usuários e apresentou uma média de 3,57 graus para que cada usuário esteja conectado a outro usuário. O experimento descobriu que os usuários ativos do site estão mais conectados que o esperado, "quebrando a teoria"no universo do site `www.facebook.com`. Entretanto, o experimento apresenta um indício de mudanças nas conexões na internet e nas iterações nas redes sociais.

Redes Livres de Escala: Barabási e Albert [Barabási e Albert, 1997] mostraram que as redes de pequeno mundo e as redes aleatórias tinham uma característica muito forte que era sua distribuição de graus formada por uma curva Poisson. Assim os nós possuíam conexões com outros nós de forma aleatória. Nas redes livres de escala os nós não são conectados de forma aleatória e sim tendem a formar uma conexão com nós da rede que já possuem um alto número de conexões [Barabási e Albert, 1997]. Essa característica é denominada de conexão preferencial que é a tendência de um novo vértice se conectar a um vértice da rede que tem um grau elevado de conexões. Diante dessa característica as redes livres de escala possuem poucos nós altamente conectados e muitos nós com baixo ou nenhuma conexão. Esses nós altamente conectados nas redes livres de escala são denominados os *hubs* da rede. Geralmente esses *hubs* são nós de grande importância na sua estrutura.

Diferentemente das redes aleatórias e de pequeno mundo as redes de livre escala são caracterizadas pela sua distribuição de grau seguindo a lei da potência no qual poucos vértices possuem altos graus e a maioria dos vértices apresentam graus baixos [Newman, 2003]. O presente trabalho, na sua seção 7.4, demonstra que o sistema Bitcoin é classificado como uma rede livre de escala proposta por [Barabási e Albert, 1997].

As redes livre de escala, por apresentarem essa topologia onde poucos nós possuem um alto grau de conexão, e muitos nós um baixo grau de conexão é alvo de grandes estudos em relação a sua tolerância a falhas. Isso porque um ataque a uma rede consiste na remoção de nós da rede com alto grau de conexão, assim tentando criar um grande impacto na sua funcionalidade. Entretanto uma falha é uma remoção aleatória de um vértice da rede. Sabendo que as redes livre de escala possuem muitos nós com baixo grau de conexão, a probabilidade que essa remoção aleatória de um nó da rede aconteça sobre um nó com pouca conexão é muito alta pois os nós com baixa conexão são a maioria nesse modelo.

Isso torna o grau dos nós das redes livre de escala uma informação importante de sua estrutura considerando o grau de um nó uma medida que determina sua importância

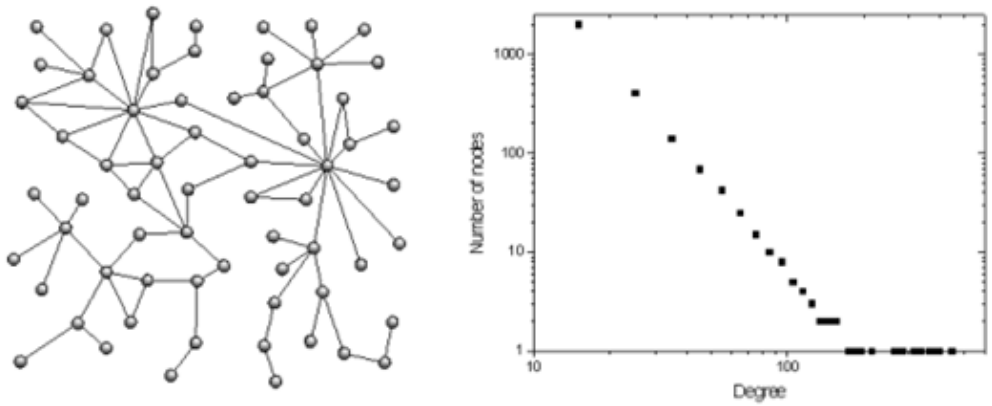

Figura 5 – Rede livre de escala e sua distribuição de graus seguindo a lei da potência [Barabási e Albert, 1997].

naquela estrutura. A informação do grau de um nó nas redes livres de escala torna a rede extremamente sensível a ataques, bastando conseguir caracterizar os graus dos nós da rede, assim tendo alvos bem discriminados para realizar o ataque e o possível dano ao seu funcionamento.

3 Sistema Bitcoin e suas características

O sistema Bitcoin surgiu em 2008, através de um documento publicado na Internet com o pseudônimo do seu autor de Satoshi Nakamoto [Nakamoto, 2008]. O documento mostra a criação de um sistema de pagamento eletrônico baseado em uma rede P2P.

3.1 Sistema Bitcoin

Bitcoin é um sistema de pagamento eletrônico descentralizado que utiliza uma rede P2P para realizar todo seu funcionamento de forma segura. É um sistema de código aberto que vem sendo aperfeiçoado desde sua criação. A invenção do sistema Bitcoin se torna revolucionária porque pela primeira vez o problema do gasto duplo pode ser resolvido sem existir uma terceira entidade centralizadora envolvida no processo. Essa característica mais uma vez é possível, pois o sistema é criado utilizando a estrutura das redes P2P, onde todos os usuários participantes realizam tarefas específicas para o funcionamento do sistema.

O sistema Bitcoin possui outras vantagens na sua utilização que chamaram a atenção de diversas empresas. O sistema usa segurança criptográfica para realizar as transações entre os usuários, taxa de transação insignificante, custo de manutenção e instalação zero. Essas características convenceram a diversas empresas a adotá-lo como um novo método de pagamento. Outras características importantes e que chamam muita atenção são: o anonimato que o Bitcoin garante entre suas transações e facilidades de privacidade. Essas características também atraíram cibercriminosos, que utilizam essas funcionalidades do sistema para realizar fraudes [Sarah Meiklejohn, 2013].

3.2 Funcionamento do sistema Bitcoin

Para o melhor entendimento do sistema Bitcoin vamos apresentar alguns conceitos utilizados na sua estrutura.

3.2.1 Endereço Bitcoin

Todo participante do sistema Bitcoin quando ingressa na rede P2P é apenas mais um nó da rede sem nenhuma identificação. Nesse momento ele somente faz parte da rede para compor sua estrutura e fortalecer sua robustez. Entretanto quando qualquer nó da rede pretende fazer alguma transação é necessário que esse nó crie uma identificação. No sistema Bitcoin essa identificação é chamada de endereço Bitcoin. Esse endereço Bitcoin é gerado pelo aplicativo cliente que pode ser instalado em qualquer computador. Juntamente com o endereço Bitcoin o usuário ganha uma chave privada. Essa chave serve para o usuário validar suas transações. O endereço de identificação é público a partir do momento

que seu dono o compartilha em qualquer lugar para recebimento de negociações.

O Endereço Bitcoin é uma *string* composta de 26 a 35 caracteres alfanuméricos que começam com os números 1 ou 3. Os endereços são criados a partir do algoritmo de chaves públicas e privadas *ECDSA*. O algoritmo gera um número *hash* da parte pública do par de chaves gerado pelo *ECDSA*. Uma garantia é que na criação de endereços Bitcoin o sistema não utiliza as letras O, I, L minúscula, e o número 0 para evitar possíveis confusões. Todos os endereços são *case sensitive* e devem ser digitados exatamente como são criados. Na figura 6 mostramos exemplos de endereços Bitcoins.

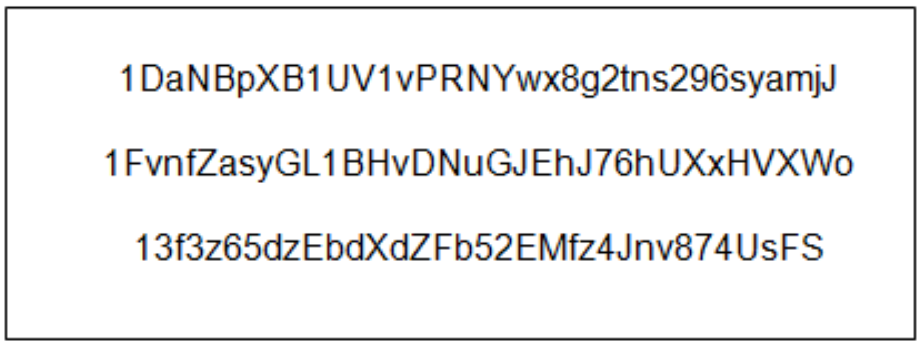

Figura 6 – Endereços Bitcoins

Um dos pontos fortes dos endereços Bitcoin é que cada usuário pode ter quantos endereços Bitcoin quiser. Essa funcionalidade que ajuda no anonimato que os usuários possuem na rede. Não existe endereço Bitcoin repetido, toda vez que o usuário que é nó da rede solicita um novo endereço é gerado um novo endereço Bitcoin totalmente exclusivo. Na criação de endereços Bitcoin não é necessário que o usuário esteja conectado a rede Bitcoin ou a Internet. Desse modo o sistemas Bitcoin facilita muito a criação de *scritps* para gerar muitos endereços aleatórios. O usuário pode ter vários endereços Bitcoin que podem ser utilizados em qualquer nova transação, ou seja o usuário pode usar para cada transação um endereço novo e diferente. Assim não vinculando um único endereço aquele usuário, essa facilidade e característica claramente ajuda no anonimato da rede.

3.2.2 Carteiras Bitcoin

A partir da identificação dos usuários através dos endereços Bitcoins, existe a preocupação de como os endereços são guardados e como não perdê-los já que qualquer usuário pode ter milhares de endereços para sua única identificação. Assim começa o conceito de carteira no sistema Bitcoin. As carteiras no sistema Bitcoin são responsáveis

por armazenar os endereços, as chaves privadas e as informações do montante de bitcoins que determinado usuário possui.

De modo bem simples as carteiras são uma coleção de chaves privadas do usuário e informações de valores. Por isso existe toda uma atenção especial pelas carteiras. Porque caso alguém tenha acesso indevido a uma carteira que não seja de sua propriedade o mesmo pode realizar qualquer tipo de transação na rede Bitcoin. No sistema Bitcoin existem vários tipos de carteiras. Existem as carteiras online, carteiras providas por hardware, carteiras locais e atualmente carteiras para dispositivos móveis. Cada uma delas com sua característica específica.

O mais importante a ressaltar é que é necessário realizar constantemente *backup* de sua carteira. Com a realização de *backups* periódicos o usuário fica protegido de qualquer falha no sistema, no seu *hardware* ou até mesmo por violação da sua carteira online, prevenindo que o usuário dono da carteira perca suas informações. Perdendo sua carteira Bitcoin o usuário perde o direito a todas suas chaves e valores guardados nessa carteira. As figuras7,8,9, e 10 apresentam alguns serviços e softwares de controle de carteiras no sistema Bitcoin.

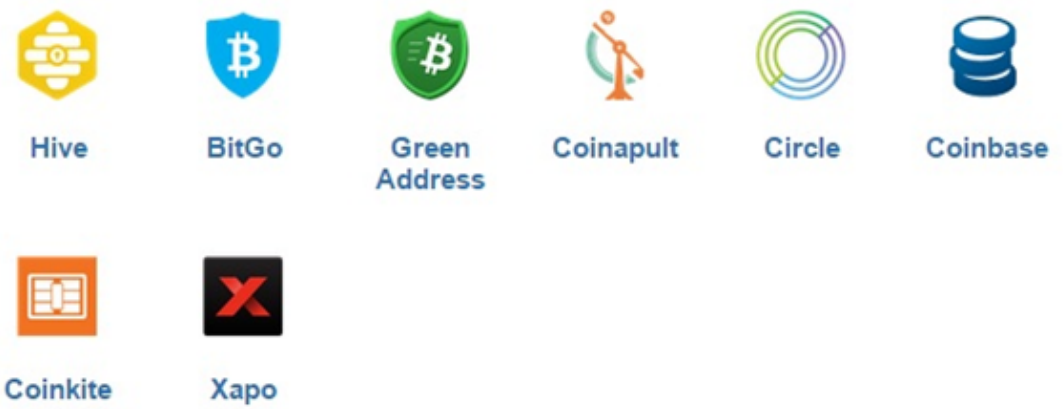

Figura 7 – Carteiras Web

Figura 8 – Carteiras providas por hardware

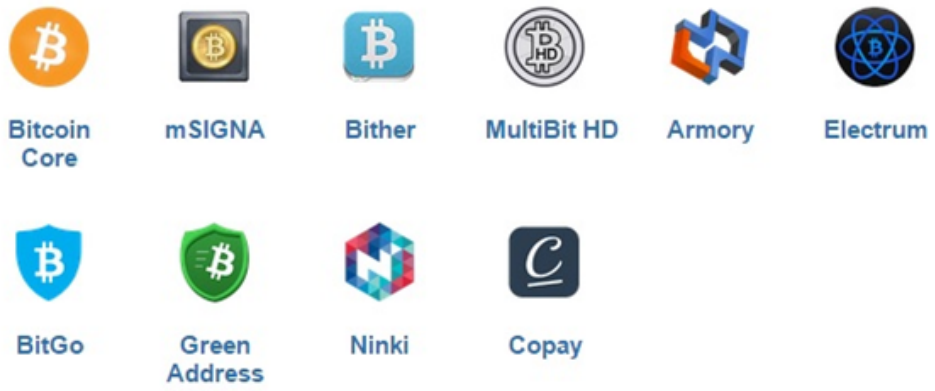

Figura 9 – Carteiras para clientes locais

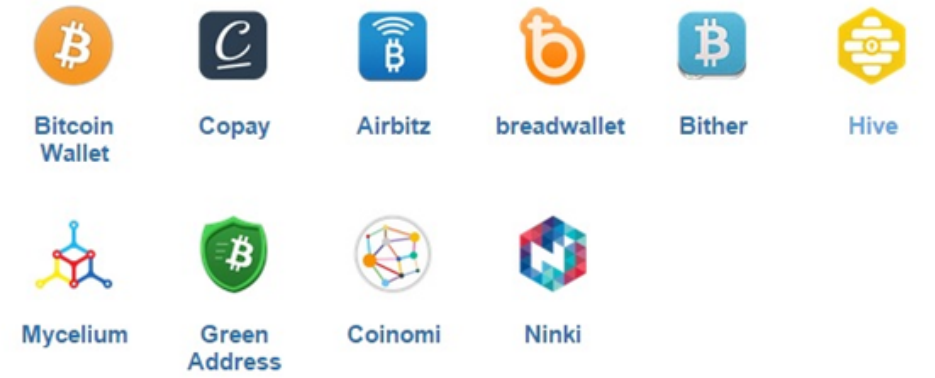

Figura 10 – Carteiras para dispositivos móveis

Assim temos muitas opções para conseguir controlar e guardar nossas informações no sistema Bitcoin. Essas informações que de fato são as mais importantes para os usuários da rede Bitcoin.

3.2.3 Blocos

Um bloco no sistema Bitcoin é uma unidade individual que compõe o *blockchain*. Os blocos contém todos os registros das transações ocorridas na rede. Todo bloco é ligado ao bloco anterior pelo número *hash* do bloco. Os blocos utilizam identificação*hash* que é calculada a partir de uma fórmula previamente estabelecida pela rede e assim aceita na rede Bitcon. O sistema de identificação *hash* utilizado pelos blocos é um sistema que torna quase impossível a manipulação dos blocos já registrados e validados na rede Bitcoin.

Os blocos são responsáveis por conter a resposta para o problema matemático gerado pela rede Bitcoin. A dificuldade do problema matemático contido em cada bloco é ajustada automaticamente pela rede. Um novo bloco só é liberado na rede Bitcoin para ser minerado após o bloco anterior ter seu problema matemático solucionado. Enquanto o

problema do bloco corrente não for solucionado a rede não gera um novo bloco para poder ser minerado. O processo de mineração de blocos veremos nas próximas seções. A tarefa de resolver o problema matemático contido nos blocos gera um prêmio para o primeiro participante da rede que resolver o problema matemático. O prêmio é uma transação de bitcon no valor de 50 bitcoins. A transação é chamada de transação recompensa ou transação *coinbase*. Essa transação é sempre a primeira transação registrada e validada no bloco atual.

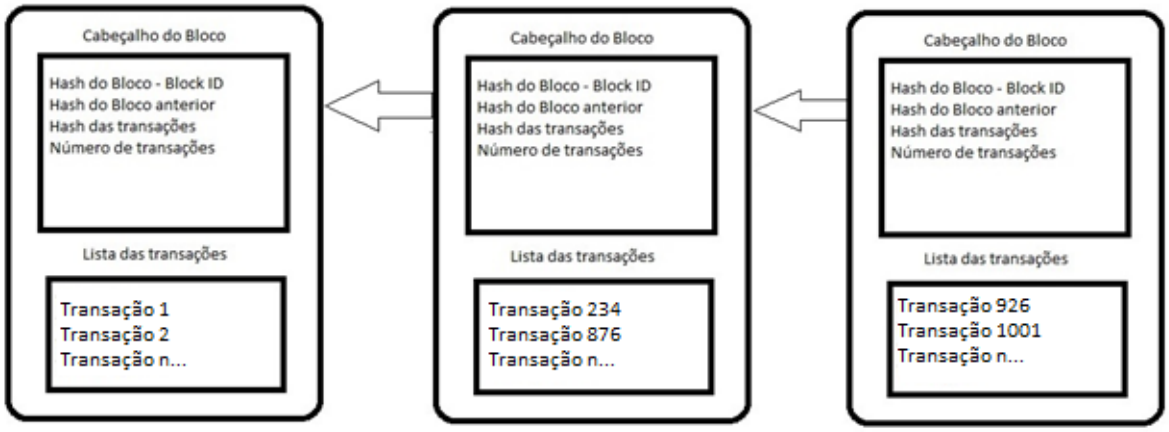

Figura 11 – Exemplo esquemático da ligação dos blocos

Com a formação de vários blocos sucessivos a rede Bitcoin cria um conceito chamado de *blockchain*. *O blockchain* é uma das partes mais importantes da estrutura da rede Bitcoin. Na próxima seção é apresentando os conceitos do *blockchain*.

3.2.4 Blockchain

Um dos componentes do sistema bitcoin de grande importância é o *blockchain*. O *blockchain* garante a segurança das informações referente às transações do sistema Bitcoin. O *blockchain* é responsável por guardar todas as informações de todas as transações já ocorridas na rede. O *blockchain* é o local onde todas as transações são disponibilizadas aos usuários da rede como se fosse um livro de transações de domínio público que não pode ser alterado. O *blockchain* nada mais é que o conjunto total de todos os blocos da rede P2P gerenciado pelo sistema Bitcoin. No *blockchain* é possível acessar as informações de todas as transações ocorridas no sistema desde seu inicio. Desse modo o bloco principal ganha o nome de *blockchain* ou bloco *Genesis*. Todo bloco do sistema Bitcoin que é encerrado e validado é ligado automaticamente ao *blockchain*, criando uma corrente de blocos já validados pela rede. O *blockchain* é disponibilizado a todos os participantes da rede, e logo quando eles entram na rede o sistema Bitcoin faz com que o novo usuário faça o *download* do *blockchain* para seu computador então o novo usuário passa a ter acesso a todas as informações das transações já ocorridas. A partir do término do *download* e sicronização

com a rede o participante passa a ser mais um ponto da rede P2P que contem uma réplica fiel de todas as informações da rede.

O *blockchain* tem o conceito de um grande banco de dados distribuídos em todos seus usuários participantes da rede, onde cada um tem uma cópia fiel dos dados. Essa característica faz com que a rede P2P do sistema Bitcoin seja classificada por uma estrutura descentralizada onde seus participantes possuem uma cópia integral da cadeia de blocos. Essa estrutura evita que a rede tenha uma base de dados centralizada como o Paypal um sistema que possui um outro tipo de estrutura [Jerry Britto e Andrea Castillo, 2013].

Outra característica importante do *blockchain* é que ele foi desenvolvido com a intenção de resolver o problema de gasto duplo. O gasto duplo se resume em controlar que uma mesma moeda não seja utilizada duas vezes por usuários diferentes ao mesmo tempo ou uma mesma moeda não seja utilizada mais de uma única vez. Nakamoto [Nakamoto, 2008], no seu documento de idealização do sistema deixa isso bem claro quando propõe que para resolver o problema do gasto duplo poderia utilizar uma rede P2P usando força de trabalho para gravar todo o histórico de transações em arquivos que dificilmente poderiam ser alterados. E que para o sistema de organização da validação e gravação do histórico das informações, bastaria uma pequena organização dos nós participantes da rede trabalhando em conjunto.

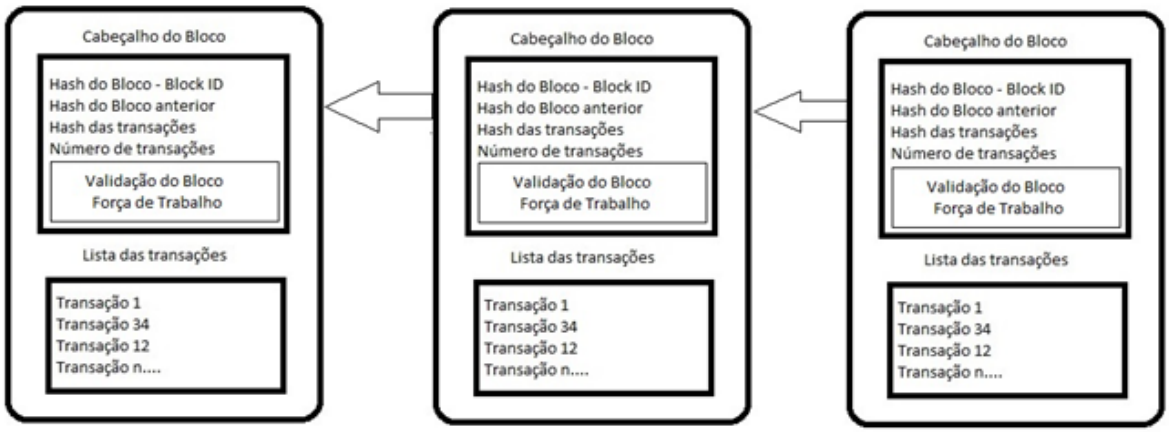

Figura 12 – Blocos prontos para o *blockchain*

A figura 12 mostra os blocos prontos para serem anexados ao *blockchain*. Anteriormente na figura 11 os blocos não tinham a informação de validação do bloco.

Na figura 13 podemos ver de forma resumida como o *blockchain* vai se formando no sistema Bitcoin. Temos o bloco 1 do sistema denominado bloco *Genesis* e suas outras ligações. Os blocos órfãos que aparecem na figura 13 representam blocos que estão aguar-

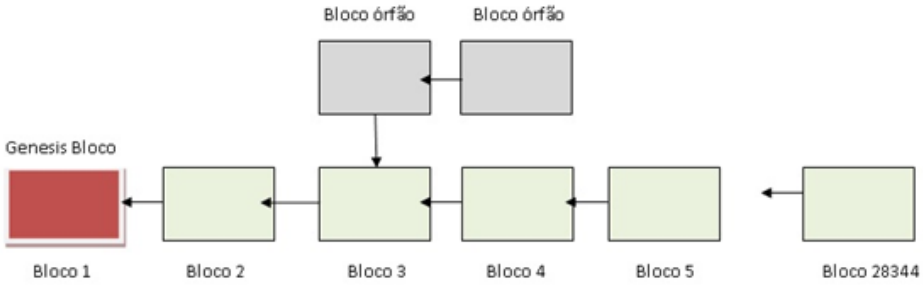

Figura 13 – Desenho esquemático do *blockchain* e suas ligações

dando sua confirmação para poderem ingressar no bloco principal.

Após o entendimento de como estão estruturados os blocos e como eles são interligados formando o *blockchain*, vamos ver na próxima seção como a rede P2P do sistema Bitcoin garante realizar a prova de trabalho para validação e criação dos blocos.

3.2.5 Mineração

O sistema Bitcoin possui partes e detalhes importantes como o *blockchain*, blocos, carteiras e os endereços. Entretanto para o funcionamento do sistema de forma segura e confiável é necessário a participação de mais um componente. Esse componente é denominado de mineradores e a mineração. O sistema Bitcoin depende da mineração para manter a integridade do *blockchain*. A mineração consiste no poder dos nós participantes em verificar todas as transações da rede e transformar o conjunto dessas transações em blocos e após a criação de um novo bloco validar esse bloco para que o mesmo faça parte do *blockchain*, [Lugin e Yong, 2015].

O processo de mineração cria novos blocos em aproximadamente 10 minutos. O controle de criação de novos blocos é realizado pelo software cliente instalado nos computadores dos participantes da rede. Os nós participantes do processo se candidatam de forma espontânea a fim de receber um prêmio caso ele seja o primeiro nó a resolver o problema computacional do bloco e fazer sua validação. Cada nó participante do processo é chamado de minerador. Todo nó participante da rede pode se candidatar para verificar e validar os novos blocos, e isso se torna essencial sabendo que a rede depende de poder computacional para a validação dos blocos.

Enquanto muitos nós da rede criam e verificam novos blocos para serem incluídos no *blockchain*, outros nós tentam resolver o problema matemático colocado no último bloco criado para que esse seja adicionado ao *blockchain* [Lugin e Yong, 2015]. O problema computacional é inserido nos novos blocos e depende da sua resolução para que os novos blocos sejam validados e incluídos no *blockchain*. É um problema matemático baseado

em solução *hash*. A dificuldade do problema é calculada automaticamente pela rede. A dificuldade é incrementada a cada 2.016 blocos baseada no tempo gasto para criação dos últimos 2.016 blocos anteriores. O valor da dificuldade é inserido em cada bloco e a partir do valor da dificuldade a rede calcula quantos bitcoins podem ser gerados em determinados períodos [Lugin e Yong, 2015].

O primeiro usuário que conseguir resolver o problema recebe um pagamento da rede por realizar essa tarefa. O processo de validação de transações, criação de blocos, validação de blocos e conexão dos blocos ao *blockchain* se torna repetitivo e faz com que a rede Bitcoin funcione de forma dinâmica. Na figura 14 podemos visualizar de forma resumida o processo de mineração.

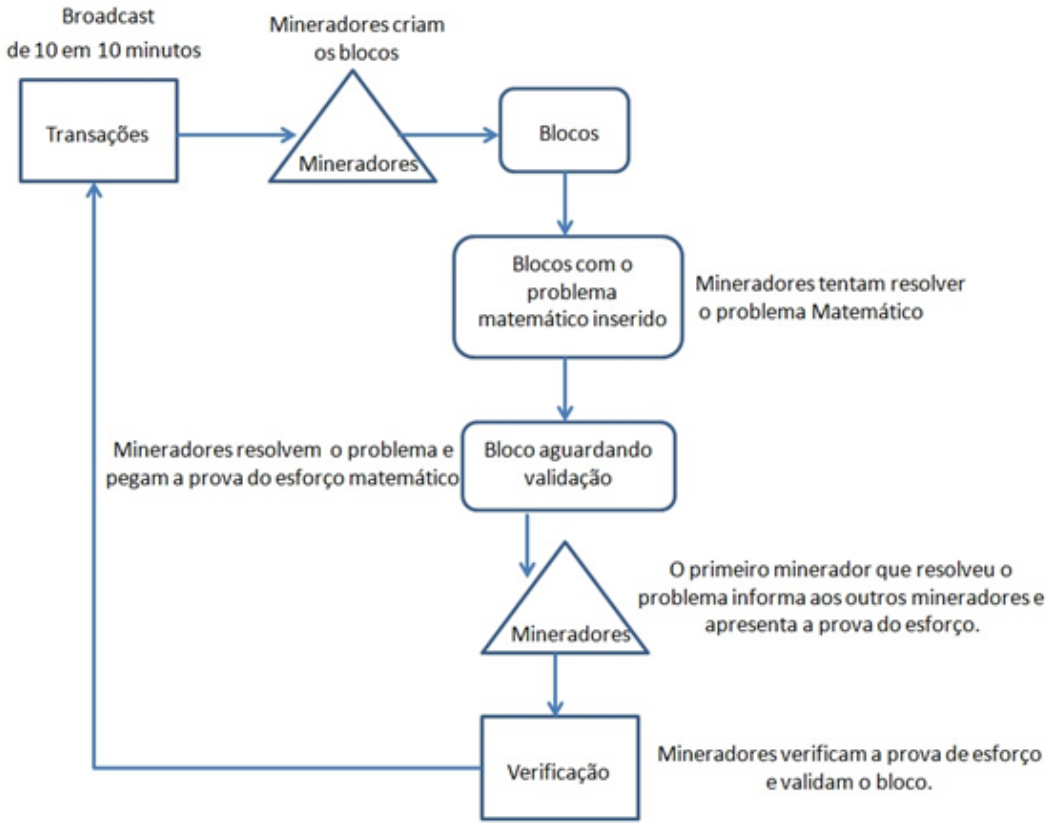

Figura 14 – Mineração no sistema Bitcoin

3.2.6 Transações

O sistema Bitcoin foi desenvolvido com o intuito de que os participantes da rede possam realizar transações financeiras sem ter uma terceira unidade regulamentadora envolvida no processo. O sistema Bitcoin tem algumas vantagens quando pensamos em transações financeiras realizadas entre dois usuários sem uma terceira entidade regulamentadora. As entidades podem ser órgãos governamentais, bancos, operadores de cartões de crédito e etc. Partindo desse princípio o sistema Bitcoin funciona basicamente

para realizar transações financeiras entre dois usuários da rede. As transações são realizadas diretamente entre um usuário A e um usuário B, ou de um usuário para vários usuários.

As transações Bitcoin são baseadas em troca de chaves criptográficas. A transação ocorre com a troca de três chaves criptográficas entre os usuários envolvidos na transação. As chaves utilizadas são: uma chave pública que pertence ao endereço do usuário que deseja enviar a transação, uma chave pública do usuário destinatário e uma chave privada do endereço do usuário que quer enviar a transação. Como todo participante da rede possui em seu computador o cliente instalado e sua carteira, a transação pode ocorrer de forma correta. São nas carteiras que estão guardadas todas as chaves privadas dos usuários. Quando o usuário A quer fazer uma transação com o usuário B, o mesmo envia sua chave pública e sua chave privada para o usuário B que por sua vez possui também uma chave pública para que ele possa receber transações de qualquer usuário. A transação ocorre quando o usuário A quer enviar para o usuário B uma moeda bitcoin, então a propriedade daquela moeda é transferida para o endereço B. A transferência de propriedade acontece quando o usuário A insere na sua carteira a chave pública do usuário B e autentica a transferência com sua chave privada. Então quando a transação é enviada ao usuário B o mesmo certifica com sua chave privada que aquela transação foi enviada para o seu usuário (sua chave pública) e assinada pelo usuário A com sua chave privada assim a transação se encerra entre os dois usuários. A partir desse ponto é necessário que os mineradores recebam a informação dessa transação através de *flooding* na rede e coloquem essa transação no bloco atual para ser validada e incorporar o *blockchain*. Todo usuário através desse processo pode realizar transferência de valores entre qualquer usuário participante da rede sem qualquer intervenção de entidades reguladoras.

Como dito anteriormente todo usuário do sistema Bitcoin possui um endereço único na rede que o identifica. Mas nada impede que o mesmo usuário tenha vários endereços, e que o mesmo faça uma transação financeira que envolva ele mesmo.

O usuário remetente precisa apenas informar o valor que deseja transferir e o endereço identificador do usuário que vai receber. Não é necessário que o usuário que irá receber a transação esteja conectado a rede. O usuário que irá receber não precisa estar conectado porque quem vai validar essa transação são os mineradores. Logo quando o usuário se conectar e atualizar seu arquivo do *blockchain* o mesmo recebe a informação que o usuário A lhe enviou algum valor em moeda bitcoin. Uma transação, após ter sido enviada para a rede, não pode ser desfeita ou cancelada.

4 Trabalhos Relacionados

O trabalho que deu a origem ao Sistema Bitcoin foi publicado na Internet para que todos tivessem acesso da idealização do funcionamento do sistema Bitcoin. O autor denominado Satoshi Nakamoto nunca foi encontrado. O trabalho que possui o estado da arte pode ser visto em [Nakamoto, 2008]. O trabalho inicial do sistema Bitcoin descreve suas características teóricas, mas em nenhum momento mostra como é feita sua implementação. No trabalho de Nakamoto, o autor explica como as transações devem ocorrer de forma segura através das chaves criptográficas e uma possível solução de como resolver o problema do gasto duplo. O trabalho também descreve como deve ser a utilização da prova de força da rede para validação das transações e dos blocos. Uma passagem muito importante do trabalho é onde o autor faz a comparação do modelo tradicional de realizar transações financeiras com o modelo que esta sendo proposto por ele no trabalho, assim criando um novo modelo de transações financeiras totalmente digitais.

Após a divulgação do trabalho inicial da criação do sistema do sistema Bitcoin outros vários trabalhos começaram a ser divulgados e publicados. Trabalhos com objetivos diferentes como: estatísticas da rede P2P que envolve o sistema Bitcoin, estudos do anonimato dos usuários entre outros pontos de interesse. [Elli Androulaki, 2013] faz um estudo das implicações do anonimato proposto pelo sistema Bitcoin. O anonimato do sistema Bitcoin sempre foi uma das grandes vantagens apontada por seus usuários. Mas como já mostrado em [Sarah Meiklejohn, 2013], também atraiu a atenção de pessoas com a intenção de realizar fraudes financeiras. [Elli Androulaki, 2013] apresenta em seu trabalho que as medidas que o sistema Bitcoin adota para tratar o anonimato de seus usuários já não são suficientes para garantir o anonimato dos usuários. O trabalho utiliza técnicas de agrupamento em ambientes menores do sistema para tentar desvendar características do usuário. [Elli Androulaki, 2013] destaca que o problema do anonimato é que qualquer usuário da rede pode ter acesso ao histórico do fluxo de transações. E a partir do estudo do fluxo de transações qualquer um pode rastrear a moeda usando técnicas apontadas no seu trabalho. Essa facilidade ocorre porque todos os participantes do sistema Bitcoin tem acesso a todas as transações através do *blockchain*. Dessa maneira é fácil obter informações referentes a rede do sistema Bitcoin tanto quanto dos seus participantes [Brugere, 2012] e [Spagnuolo, 2013].

[F.Reid e M. Harrigan, 2011], mostram em seu trabalho que o sistema Bitcoin não garante mais o total anonimato de seus usuários. [F.Reid e M. Harrigan, 2011] apontam que um dos problemas da quebra do anonimato do sistema Bitcoin da-se ao fato que todos podem retirar informações do *blockchain*. Desse modo qualquer pessoa pode recriar o grafo de transações da rede e o grafo de usuários da rede. No trabalho os autores demonstram

que montando o fluxo de transação de bitcon entre dois usuários ou mais é possível extrair sua identificação. O trabalho apresenta ainda outras formas de realizar a identificação dos usuários do sistema.

Os trabalhos anteriores aqui mencionados citaram que o sistema Bitcoin possui dois tipos de grafos importantes que compões seu funcionamento. Esses grafos são denominados grafo de usuários(nós) e o grafo de transações(arestas). Através do estudo desses grafos podemos reconstruir o fluxo de onde uma moeda saiu e para onde ela foi assim identificando o usuário que emitiu o pagamento e o usuário que recebeu o pagamento. [D. Ron e A. Shamir, 2013] demonstram em seu trabalho que, mais uma vez através do estudo do *blockchain*, que é público, é possível retirar informações interessantes dos usuários do sistema. Os autores fazem a cópia completa do *blockchain* e analisam diversas propriedades estatísticas associadas às transações. Essas informações apontadas no trabalho são: como os usuários gastam seus bitcoins, o saldo de bitcoins dos usuários, como os usuários movem bitcoins entre seus diversos endereços para manter sua privacidade e etc.

O sistema Bitcoin possui diversas variáveis e características que podem ser estudas e analisadas. Um trabalho interessante que faz uma caracterização do tipo de usuário que a rede possui é apresentando por [Sarah Meiklejohn, 2013]. O trabalho identifica vários participantes do sistema e os separa em grupos. Os usuários identificados no trabalho são usuários com forte atuação no sistema. O sistema Bitcoin possui alguns usuários específicos como os mineradores, as carteiras, vendedores, casas de câmbio, casas de jogos e outros usuários. O trabalho apresenta duas heurísticas de como agrupar esses usuários e defini-los, mostrando mais uma vez que o anonimato no sistema não é tão forte como supostamente foi apresentado. O trabalho também caracteriza variáveis referente a rede do sistema como: média de transações, menores transações, transações recebidas e um balanço de quanto que cada usuário transaciona com os usuários categorizados pelo trabalho.

Apesar do sistema Bitcoin ser uma nova tecnologia muitos pesquisadores se interessaram por ela, pois o sistema tem um potencial inovador, revolucionário e robusto capaz de se tornar um meio de realizar transações financeiras totalmente digital descentralizada. No estudo dos trabalhos relacionados podemos perceber que ainda temos poucos trabalhos na área mas já temos bons trabalhos que tratam do assunto. Atualmente a importância do tema se mostra bastante forte quando o MIT cria um laboratório de pesquisa voltado totalmente para o estudo dos sistemas de cripto moedas. O laboratório denominado Digital Currency Initiative. O laboratório conta com um dos principais desenvolvedores do protocolo Bitcoin, Gavin Andresen. O laboratório tem como seu principal ponto de pesquisa as questões de segurança, estabilidade, escalabilidade, privacidade e economia.

No presente trabalho, nós realizamos a caracterização na rede P2P do sistema Bitcoin. Analisamos a rede em seu funcionamento sazonal diário tanto quanto realizamos a aplicação de métricas relacionadas a redes complexas para entender em qual modelo de rede complexas o sistema Bitcoin se enquadra. O trabalho apresenta uma forma de descobrir usuários participantes do sistema Bitcon de alta conectividade. Através da alta conectividade desses usuários descobrimos pontos importantes na rede do sistema Bitcoin. Nos próximos capítulos apresentamos a metodologia da captação dos dados, extração dos dados e modelagem dos dados para a obtenção das informações. Em uma segunda parte após os dados modelados realizamos a caracterização do funcionamento do sistema baseado no seu funcionamento diário, mensal, apresentando gráficos do funcionamento do sistema. A última caracterização proposta é a utilização das métricas de redes complexas para apresentar a topologia estrutural da rede e sua importância.

5 Metodologia e Modelagem

Esse capítulo descreve a metodologia adotada para a retirada dos dados do sistema Bitcoin e logo após a realização das análises e seus resultados. Após apresentar a metodologia para a retirada dos dados é apresentado como os dados foram modelados e armazenados para utilização no estudo do funcionamento da rede em relação às suas variáveis de funcionamento diário e estrutura.

5.1 Extração dos dados do Sistema Bitcoin

Para a extração dos dados do sistema Bitcoin utilizamos nesse trabalho o cliente Bitcon próprio para utilização em servidores. O cliente é utilizado sem interface gráfica e roda no modo *background* como um *daemon*. Atualmente qualquer versão dos clientes oficiais da rede Bitcoin podem ser baixados no site do sistema: `https://bitcoin.org/pt_BR/download`. A instalação do cliente é obrigatória para iniciar a cópia dos dados necessários que serão objeto de estudo das características da rede. Como apresentado anteriormente qualquer novo usuário que se conecta a rede realiza automaticamente uma cópia fiel do *blockchain*. A cópia contém todo o registro das informações da rede. Após realizar o *download* do cliente e fazer a instalação o primeiro procedimento que acontece é a sincronização do novo usuário com a rede Bitcoin. Esse processo é demorado, pois o novo participante realiza o *download* completo da base de dados para o seu computador. Para a extração dos dados não é necessário a utilização do cliente com interface gráfica, pode-se utilizar um cliente com interface mais amigável para a realização do *download* do *blockchain* e realizar a sincronização com a rede. A figura 15 é o exemplo do cliente oficial do sistema Bitcoin no procedimento de sincronização com rede. No exemplo utilizamos um cliente com interface gráfica para melhor visualização.

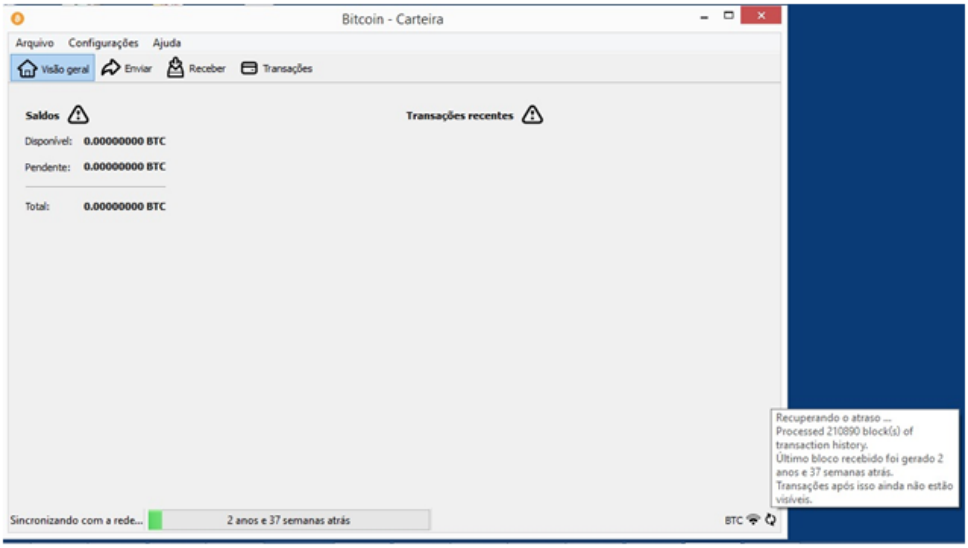

Figura 15 – Client Bitcoin original sincronizando com a rede

Após o término da sincronização com a rede teremos no computador todo o *blockchain* disponível para extração dos dados. Nesse momento o computador estará sincronizado com a rede Bitcoin e tem disponível de forma bruta todas as informações da rede Bitcoin.

Na próxima seção é apresentado o processo de *parser* realizado sobre o *blockchain* onde modelamos esses dados brutos extraídos em dados armazenados de forma compreensível para análises e estudos.

5.2 Realizando Parsing no Blockchain

Para realizar o *parser* é preciso ter no diretório do cliente Bitcoin os arquivos *blocks* os quais formam o *blockchain*. Nestes arquivos estão todas as informações referentes à rede do sistema Bitcoin. Nas pesquisas realizadas descobrimos duas opções de *parser*. O primeiro disponível no endereço `https://github.com/znort987/blockparser`. Entretanto após uma maior pesquisa foi utilizado o parser disponível no endereço `https://github.com/mikispag/bitiodine/tree/master/deploy`. O *parser* escolhido é utilizado em [Spagnuolo, 2013], onde é apresentado melhorias em relação ao *parser* antigo proposto por *znort987*. Essas melhorias são relacionadas a desempenho e forma de armazenamento dos dados. A versão do *parser* apresentado por [Spagnuolo, 2013] é apenas um modificação do *parser* original proposto por *znort987*.

O *parser* faz a leitura de todos os arquivos *blocks.dat* que estão dentro do diretório do cliente Bitcoin e transforma essas informações em informações modeladas para nosso entendimento. O resultado da utilização do *parser* é a criação de uma base de dados montada em *SQLite3*. A partir desse banco de dados relacional criado pelo *parser* é possível a extração das informações das características básicas da rede.

No término da execução do *parser* proposto por [Spagnuolo, 2013], são gerados os seguintes arquivos de formato txt: *blocks.txt, txin.txt, txout.txt e tx.txt*. Esses arquivos são as fontes dos dados para realizar a população do banco de dados. O *parser* também cria o arquivo *blockchain.sql*. O arquivo *blockchain.sql* contém a estrutura do banco de dados para criação de seu modelo físico. Após a criação da estrutura física do banco de dados basta agora alimentar o banco de dados através dos arquivos *txt* criados anteriormente.

Quando o banco de dados estiver populado a única necessidade é a execução de comandos *SQL* para a obtenção das informações básicas da rede Bitcoin. A figura16 mostra o modelo relacional do banco de dados criado pelo parser proposto por [Spagnuolo,2013].

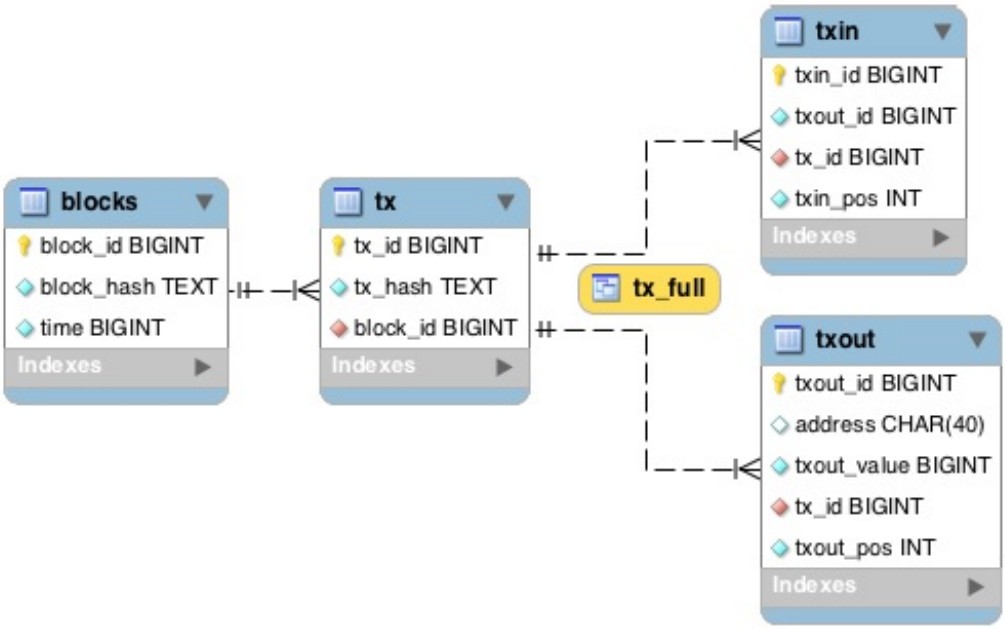

Figura 16 – Modelo relacional proposto por [Spagnuolo, 2013]

Através desse modelo as informações como: quantidade de blocos, tempo de *hash*, identificação de transações, identificação de usuários, valores de entrada e saída de bitcoins podem ser obtidas através do banco de dados modelado.

No *parser* proposto por Spagnuolo é criada uma *view* que detalha uma transação por completo. A figura 17 mostra a *view* proposta por [Spagnuolo, 2013].

```
CREATE VIEW tx_full AS
SELECT blocks.time, tx.tx_hash, tx.tx_id, txout.address, txout.txout_value
FROM txout LEFT JOIN tx ON (tx.tx_id = txout.tx_id) LEFT JOIN
    blocks ON (tx.block_id = blocks.block_id);
```

Figura 17 – *View* principal proposta por [Spagnuolo, 2013]

A partir da *view* principal proposta por [Spagnuolo, 2013] esse trabalho deriva todas as consultas realizadas no banco de dados.

Então, logo que o banco de dados esteja criado e populado, é possível a extração dos dados básicos da rede Bitcoin através da execução de instruções *SQL* obedecendo ao relacionamento como visto na figura 16

Essa seção apresentou como obter dados básicos da rede Bitcoin através da realização de *parsing* e modelagem dos dados em um banco de dados *SQLite3*. Através de instruções

```
select blocks.time, txout.tx_id, txout.txout_value, txout.address, txin.tx_id,
txin.txout_id from txout join txin on (txin.tx_id=txout.tx_id)LEFT JOIN tx
ON (tx.tx_id = txout.tx_id) LEFT JOIN blocks ON (tx.block_id =
blocks.block_id) where blocks.time between 1383271200 and 1386208800
```

Figura 18 – Exemplo de busca realizada na base de dados.

SQL observando o relacionamento modelado no banco de dados é possível a extração de informações relevantes do funcionamento do sistema Bitcoin. Na próxima seção será apresentado como obter informações da rede Bitcoin em relação a sua estrutura.

5.2.1 Extraindo dados para análise da estrutura do sistema Bitcoin

Na seção anterior foi apresentado como realizar a extração de dados do *blockchain* utilizando a modelagem dos dados através de banco de dados, onde com, a execução de instruções *SQL*, é possível obter informações do funcionamento do sistema Bitcoin. Entretanto para uma análise da estrutura da rede do sistema Bitcoin foi necessário utilizar *scripts* feitos em *Python* e transformar as informações obtidas em modelos de grafos. Em [Spagnuolo, 2013] foi desenvolvido dois *scripts* em *Python* os quais transformam as informações contidas no *blockchain* em arquivos com extensão *.dat* e no formato *Pickle*, onde esses arquivos podem ser lidos pela linguagem *Python*. Esse modelo de retirada dos dados é necessário porque o objetivo é obter informações da estrutura da rede. A rede do sistema Bitcoin é uma rede P2P com milhões de nós e arestas. Para realizar a leitura desses milhões de nós e arestas foi necessário a utilização dos dois *scripts* criados por [Spagnuolo,2013]. Os *scripts* criam duas redes paralelas ao sistema bitcoin. Os *scripts* extraem a rede das transações do sistema (arestas) e a rede dos usuários(nós) participantes do sistema. Após a obtenção dessas duas redes paralelas é possível o estudo da estrutura da rede utilizando *scripts* criados em *Python*.

Uma das contribuições do trabalho foi a melhoria dos dois *scritps* criados por [Spagnuolo, 2013]. Anteriormente para conseguir informações da rede era necessário ler todos os arquivos do *blockchain* e fazer uma análise geral de todo o funcionamento da rede desde seu inicio até o dia atual da base. Após a melhoria dos dois *scripts* agora é possível estudar períodos distintos na rede do sistema Bitcoin assim facilitando análises pontuais e economizando tempo. Agora com a aplicação dos *scripts* criados e melhorados obtemos arquivos mais resumidos e contendo apenas as informações as quais queremos analisar.

Após os resultados gerados é necessário utilizar *scripts* criados em *Python* para

a leitura das informações contidas nos arquivos. Com essa necessidade pontual criamos um *script* em *Python* para a extração de dados estruturais da rede do sistema Bitcoin. O *script* foi utilizado para obter as informações para a análise através das métricas utilizadas no trabalho. No capítulo 6 do trabalho será apresentado a análise da dinamicidade do sistemas Bitcoin.

6 Análise da Dinamicidade do Sistema Bitcoin

Apresentamos nesse capítulo a análise da dinamicidade do sistema Bitcoin baseado em suas variáveis de funcionamento diário. Os dados analisados são dados extraídos do *blockchain* através da modelagem apresentada no capítulo 5.

6.1 Análise das Variáveis Diárias do Sistema Bitcoin.

Com a base de dados modelada, é possível retirar informações de cada bloco individualmente ou como um todo. O sistema Bitcoin é formado essencialmente de transações realizadas entre dois usuários previamente desconhecidos. Com o estudo do número de transações pode-se observar características sazonais do sistema Bitcoin e suas alterações.

Os dados analisados para caracterização das transações são dados referentes aos meses de Outubro, Novembro e Dezembro/2013. As análises realizadas referentes aos três meses ocorre por interesse de verificar o comportamento do sistema baseado em acontecimentos externos que podem afetar as características do funcionamento do sistema Bitcoin. Em Outubro e Novembro de 2013 o FBI fechou o site denominado *Silk Road*. O site *Silk Road*, teve sua criação em Janeiro/2011 e foi fechado em Outubro/2013. O *Silk Road* ficou amplamente conhecido por realizar vendas de qualquer tipo de produto e serviço ilegal desde drogas até armas. O *Silk Road* exclusivamente realizava suas transações com a moeda digital Bitcoin. Também não é um site da Internet comum e sim um site da *Deep Web*, assim criando dificuldade para o rastreamento de transações e identificação de usuários.

Fizemos a análise do período entre os meses de Outubro, Novembro e Dezembro/2013 a fim de conseguir capturar possíveis alterações no sistema devido ao acontecimento do fechamento do site *Silk Road*. Através do período escolhido podemos captar as modificações das variáveis do sistema Bitcoin e fazer as análises do seu funcionamento.

Muitos usuários e alguns veículos da mídia chegaram a vincular o sucesso do sistema Bitcoin diretamente à utilização da moeda em transações através do *Silk Road*. Entretanto, após a análise das transações ocorridas na rede nesse período, verifica que a rede não sofre nenhum grande impacto logo após o fechamento do site *Silk Road*.

A tabela 1 apresenta o levantamento de todas as transações ocorridas nos meses de Novembro desde o surgimento do sistema Bitcoin. Nota-se um comportamento de crescimento de utilização do sistema levando em consideração o número de transações realizadas nos meses de Novembro no período de 6 anos.

A tabela 2 faz uma comparação do número de transações mensais realizadas pelo sistema Bitcoin um mês antes do fechamento do *Silk Road* e um mês após o fechamento

Mês	Número Total de Transações Mês
Novembro/2009	2.228
Novembro/2010	63.369
Novembro/2011	168.629
Novembro/2012	942.575
Novembro/2013	1.959.041
Novembro/2014	2.512.399

Tabela 1 – Total de Transações dos meses de Novembro

Mês	Número Total de Transações Mês
Outubro/2013	1.645.153
Novembro/2013	1.959.041
Dezembro/2013	1.941.525

Tabela 2 – Número de transações mês antes e após o fechamento do *Silk Road*

do site. Observa-se que após o fechamento do site, as transações realizadas pelo sistema Bitcoin quase se mantém com o mesmo volume. Logo é notável que o sistema Bitcoin não estava totalmente vinculado a transações ilegais baseadas em sites existentes na *Deep Web*. Através da análise dos meses de Outubro, Novembro e Dezembro de 2013 baseado no número de transações realizadas mensalmente pelo sistema Bitcoin é possível detectar que a rede não segue nenhum tipo de padrão em seu funcionamento mensal. Isso demonstra que o sistema Bitcoin tende a possuir um comportamento de funcionamento totalmente imprevisível durante seu funcionamento. Onde o número de transações realizadas mensalmente ocorrem de forma totalmente independente de qualquer tipo de acontecimento externo ao sistema. O sistema não segue um comportamento previsível onde durante os dias de semana poderia existir mais transações e aos finais de semana a rede poderia ter um volume menor de transações.

Observando essa sazonalidade da rede as tentativas de fraudes no sistema podem ocorrer a qualquer período do seu funcionamento. Pois sabendo que o volume de transações mensal é uma variável que não tem um comportamento previsível o rastreamento de transações se torna difícil em qualquer período do funcionamento do sistema. Os gráficos 19, 20 e 21 mostram essa sazonalidade da rede acontecendo nos meses de Outubro, Novembro e Dezembro de 2013.

O gráfico 22 ilustra que não existe nenhum padrão de funcionamento diário do sistema Bitcoin entre os meses analisados. Também demonstra que mesmo com o fechamento da *Silk Road* o sistema Bitcoin manteve sua imprevisibilidade de funcionamento baseado em número de transações diárias. Onde muitos imaginavam que a rede poderia sofrer uma grande queda nas suas transações diárias a rede se permanece estável como contabilizado na tabela 2 e também visualizado no gráfico 22.

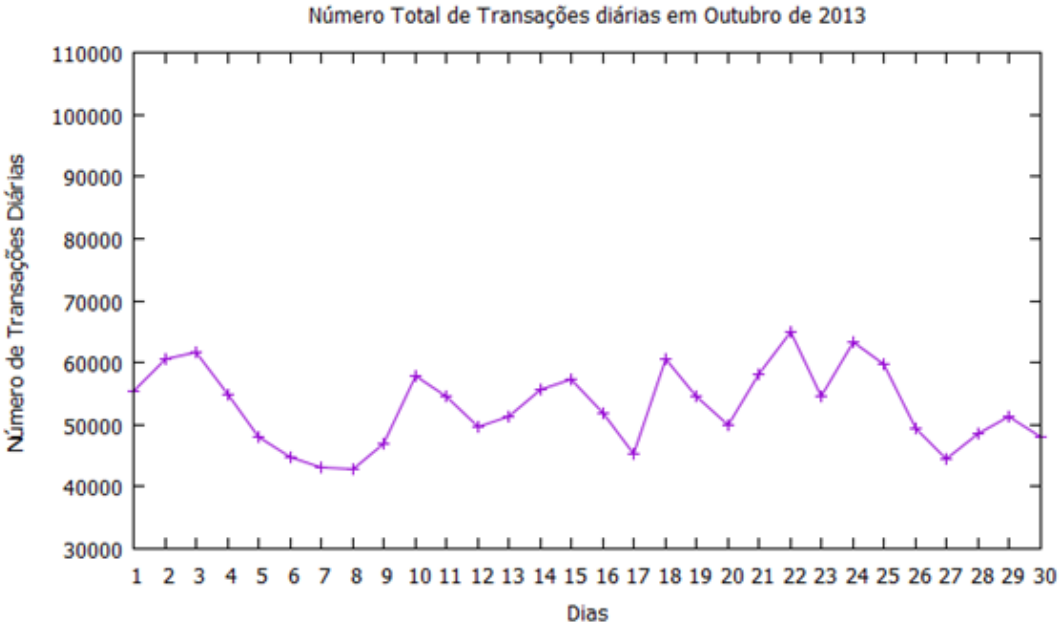

Figura 19 – Transações Diárias Outubro de 2013

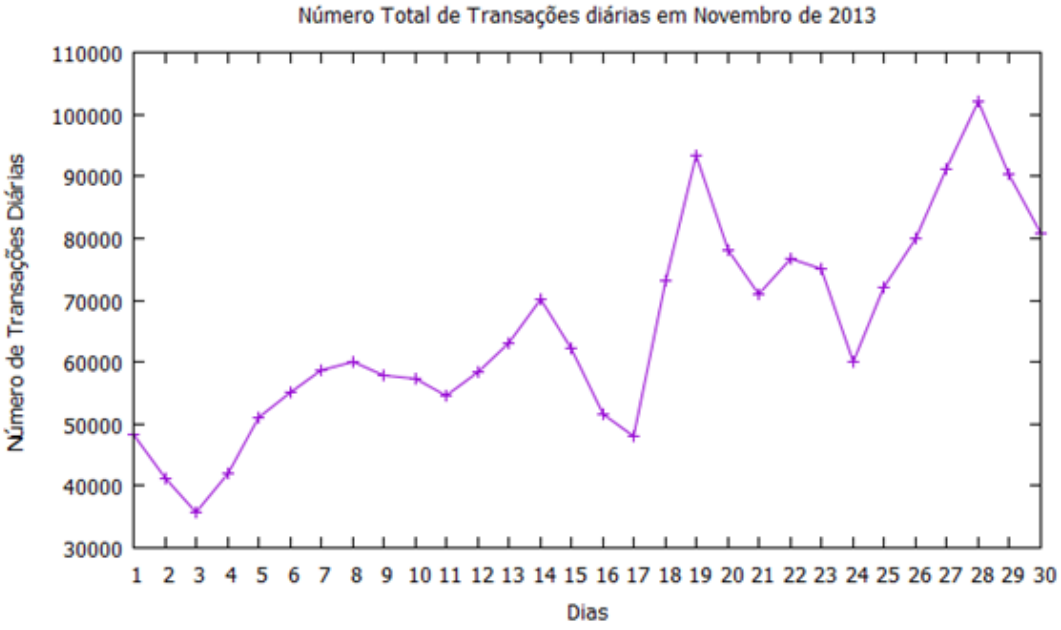

Figura 20 – Transações Diárias Novembro de 2013

6.2 Volumes Transacionados Diariamente

As análises realizadas na seção anterior mostram que o sistema Bitcoin não apresenta um funcionamento previsível mediante sua variável que se refere ao número de transações diárias. Então é realizada a comparação entre número de transações diárias e o volume transacionando. A comparação é a tentativa de descobrir se existe relação entre número de transações e volume de bitcoins transacionados. Partindo desse ponto, caso aconteça algum

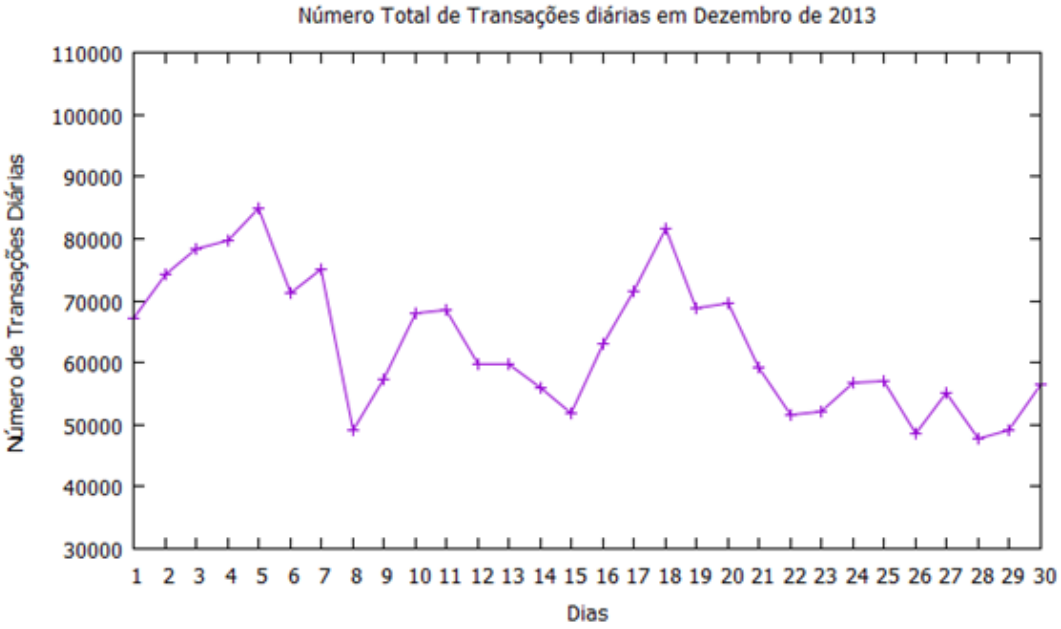

Figura 21 – Diárias Dezembro de 2013

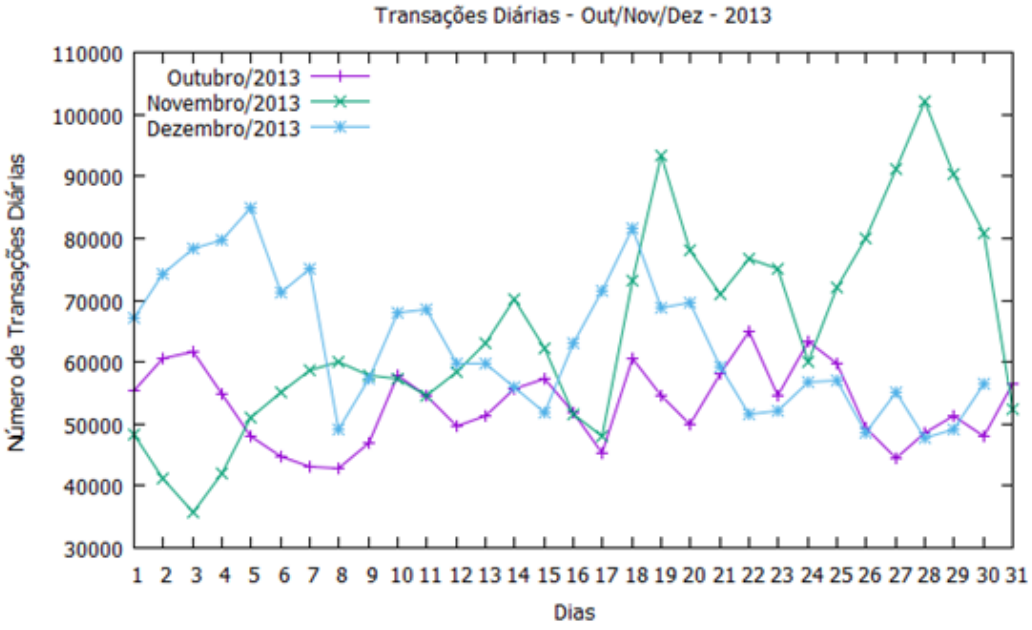

Figura 22 – Diárias-Out/Nov/Dez - 2013

evento externo ao sistema bitcoin, que possa fazer com que seus usuários movimentem suas moedas a rede poderá sofrer uma demanda maior de volume de bitcoins movimentados. A análise referente aos volumes transacionados tem como base os mesmos meses já avaliados nas transações diárias.

A tabela 3 mostra um aumento no volume de bitcoins transacionados no mês de novembro. Em Outubro de 2013 o site *Silk Road* foi fechado pelo FBI. Mais uma vez nota-se

Mês	Volume Total de bitcoins Transacionados no mês
Outubro/2013	5.830.171(BTC)
Novembro/2013	7.987.325(BTC)
Dezembro/2013	5.574.619(BTC)

Tabela 3 – Volume Total de bitcoins Transacionados Mês.

que o bitcoin não estava totalmente vinculado a atividade ilegal exercida pelo *Silk Road*. Entretanto o fechamento do *Silk Road* causou um impacto no volume transacionado no mês de Novembro de 2013. Fazendo com que os usuários do sistema Bitcoin movimentassem suas moedas, seja realizando as últimas compras antes do fechamento do site ou o movimento dos próprios administradores fazendo com que seus bitcoins fossem transferidos.

Os gráficos 23, 24 e gráfico25 demonstram a relação entre número de transações diárias e o volume de bitcoin transacionados.

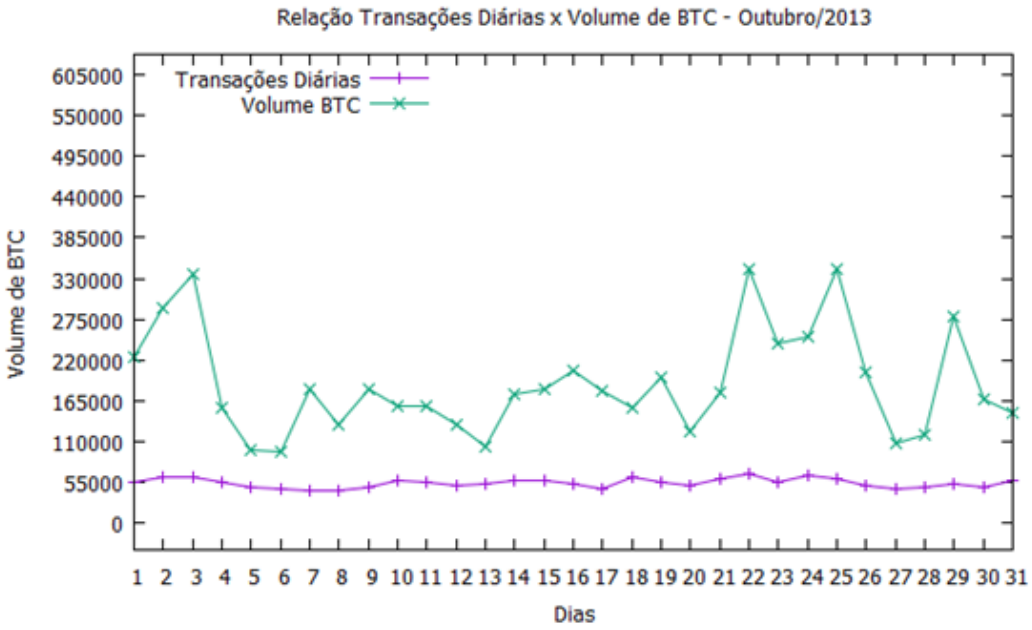

Figura 23 – Relação Transações Diárias x Volume de bitcoins-Outubro/2013

A análise dos gráficos 23, 24 e gráfico 25 mostra que o volume de bitcoins transacionados não tem uma relação com o número de transações diárias. Nos meses analisados as transações diárias permaneceram com uma média de 55.000 transações diárias enquanto o volume de bitcoins se alterna. Já o número de transações mantém uma constância.

É notável que durante o mês de novembro de 2013 o volume de bitcoins transacionados é superior que os demais meses. Assim cria-se uma relação entre o *Silk Road* e o volume de bitcoin transacionado. Diferentemente da variável número de transações diárias que já foi comparada nesse trabalho e apresentou uma característica de estabilidade mesmo com o *Silk Road* em funcionamento e também após o seu encerramento. Assim

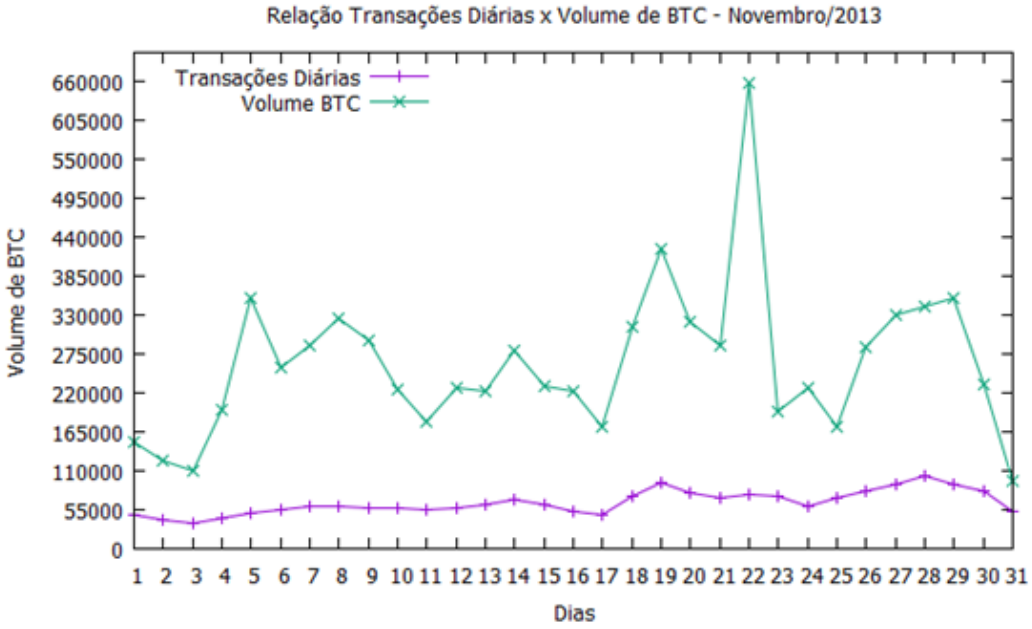

Figura 24 – Relação Transações Diárias x Volume de bitcoins-Novembro/2013

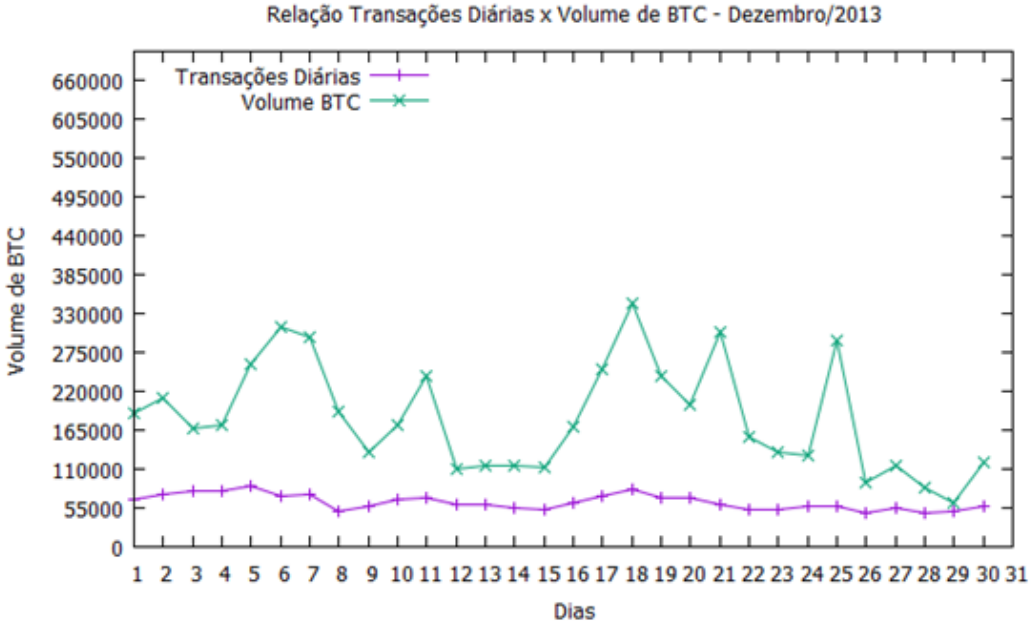

Figura 25 – Relação Transações Diárias x Volume de bitcoins-Dezembro/2013

quando é analisado o volume de bitcoins transacionados o fechamento do site *Silk Road* fez com que o volume de bitcoins transacionados aumentasse. Isso pode ocorrer devido aos valores que os serviços do *Silk Road* disponibilizavam. Então a variável transações diárias tem sua característica de provável estabilidade enquanto a variável volume de bitcoins transacionados tem sua característica como dependente de fatores externos. Levando em consideração que quando o site *Silk Road* foi fechado houve um aumento no volume de

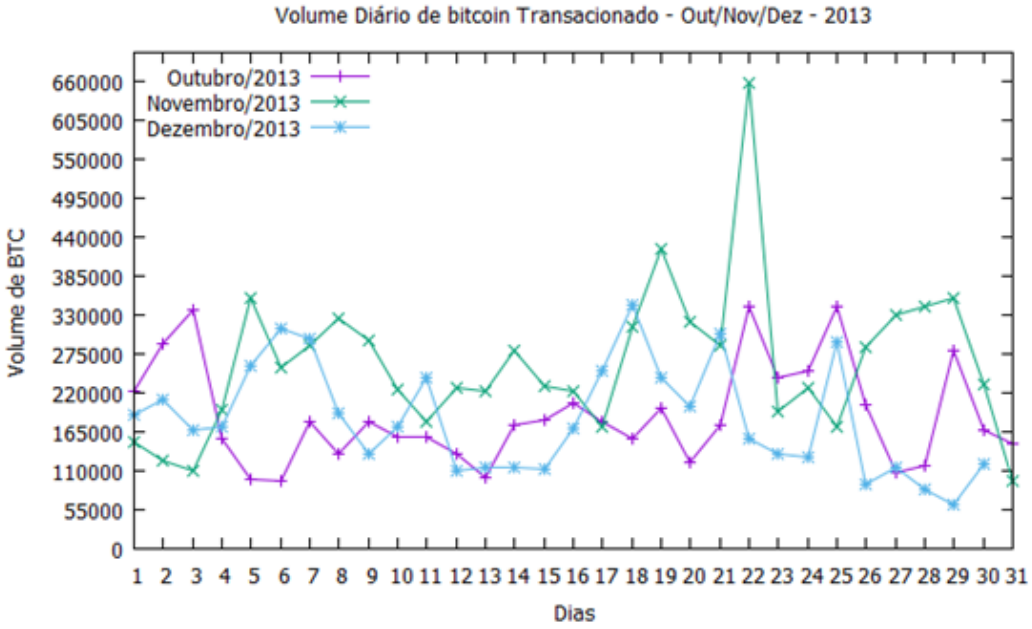

Figura 26 – Volume Diário de bitcoin Transacionando-Out/Nov/Dez-2013

bitcoins transacionados.

6.3 Usuários participantes no Sistema Bitcoin

Nas seções anteriores foram analisadas duas variáveis que apresentam volume de bitcoins e número de transações. Analisando as duas variáveis demonstrou-se alguns indícios de comportamento do sistema Bitcoin. Agora o interesse é analisar o componente que faz com que a rede cresça e seja dinâmica. Por isso nessa seção a análise é feita com relação aos usuários participantes no sistema. Na rede P2P que dá suporte ao Bitcoin esses usuários são os nós da rede. Os usuários do sistema Bitcoin são identificados através de um endereço único. Cada usuário pode ter quantos endereços quiser. Essa técnica de um único usuário ter muitos endereços é utilizada para dificultar o rastreamento de transações.

Para continuar o paralelo com o fechamento da *Silk Road* os dados analisados são dos meses de Outubro, Novembro e Dezembro de 2013. No capítulo 5 o trabalho apresenta a metodologia para a extração das informações utilizadas. Através da tabela TXOUT modelada no banco de dados proposto por [Spagnuolo, 2013] é possível a retirada dos endereços dos usuários participantes na rede.

A tabela 4 mostra que os endereços únicos Bitcoin mesmo com o fechamento da *Silk Road* continuou crescendo. Mais um indício que o sistema não era totalmente ou fortemente vinculado ao *Silk Road*. Esse número de endereços claramente tem tendência

Mês	Usuários Únicos
Outubro/2013	2.155.880
Novembro/2013	3.437.753
Dezembro/2013	3.850.811

Tabela 4 – Endereços Bitcoins únicos.

em crescimento mesmo ocorrendo algum acontecimento externo ao funcionamento do sistema Bitcoin. Essa característica ocorre devido a tentativa de dificultar o rastreamento de transações e identificação de usuários, sabendo que qualquer usuário pode ter quantos endereços desejar. No gráfico 27 essa característica quando é analisada diariamente se torna mais fácil de visualizar.

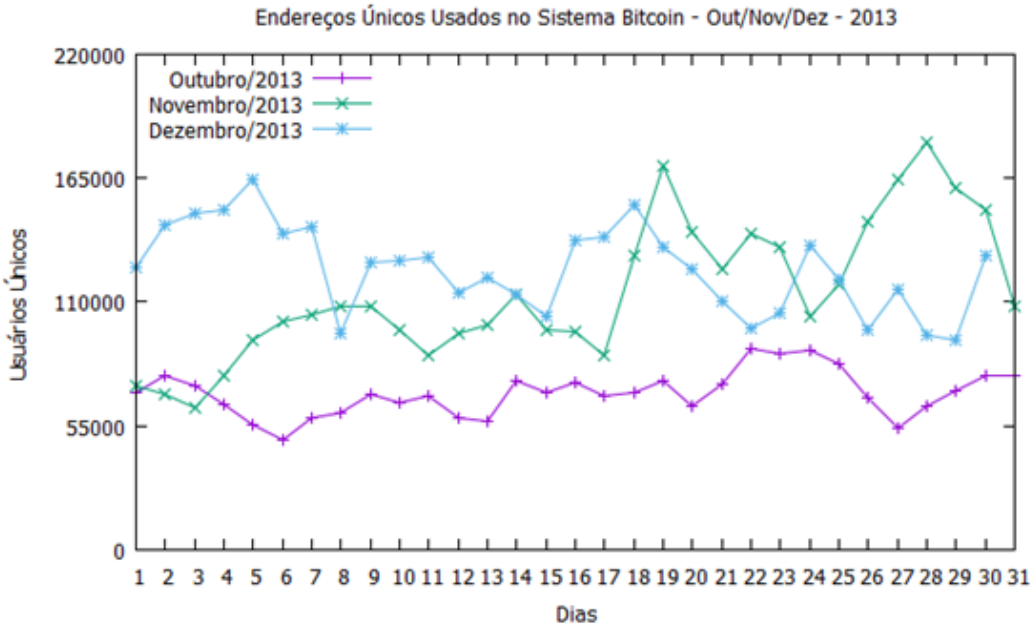

Figura 27 – Endereços Únicos Usados no Sistema Bitcoin-Out/Nov/Dez-2013

No gráfico 27 é possível perceber um aumento de endereços únicos criados mensalmente. O gráfico revela dias que podem ser levados como dias de importância para se realizar investigações mais detalhadas. No gráfico 27 destacamos os dias 19 de Novembro de 2013, 28 de Novembro de 2013 para dias que tem elevado número de endereços únicos de Bitcoins utilizados. Fica evidenciado mais uma vez que no período do fechamento da *Silk road*, os usuários do sistema Bitcon, criaram vários novos endereços para realizar a movimentação de suas moedas e dificultar seu rastreamento ou sua identificação. Nos gráficos 28, 29 e 30 é realizado uma melhor análise comparando número de endereços únicos de Bitcoins com o volume transacionado.

Os gráficos 28, 29 e 30 apresentam momentos distintos do sistema Bitcoin. Uma relação interessante que é retirada dessa análise individual, é que levemente o número

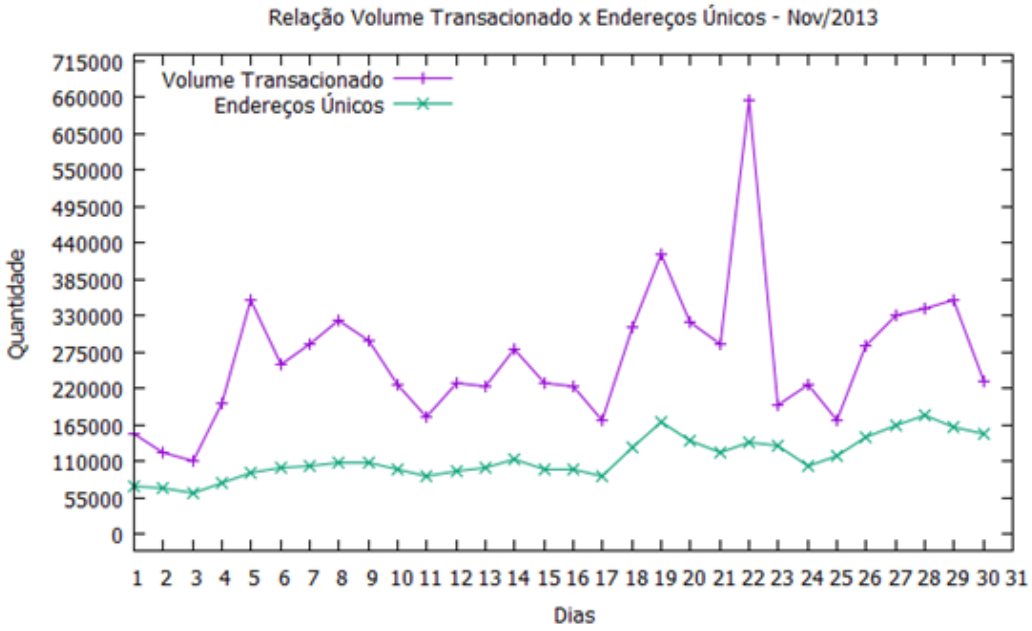

Figura 28 – Comparação Volume Transacionado x Endereços Únicos-Nov/2013.

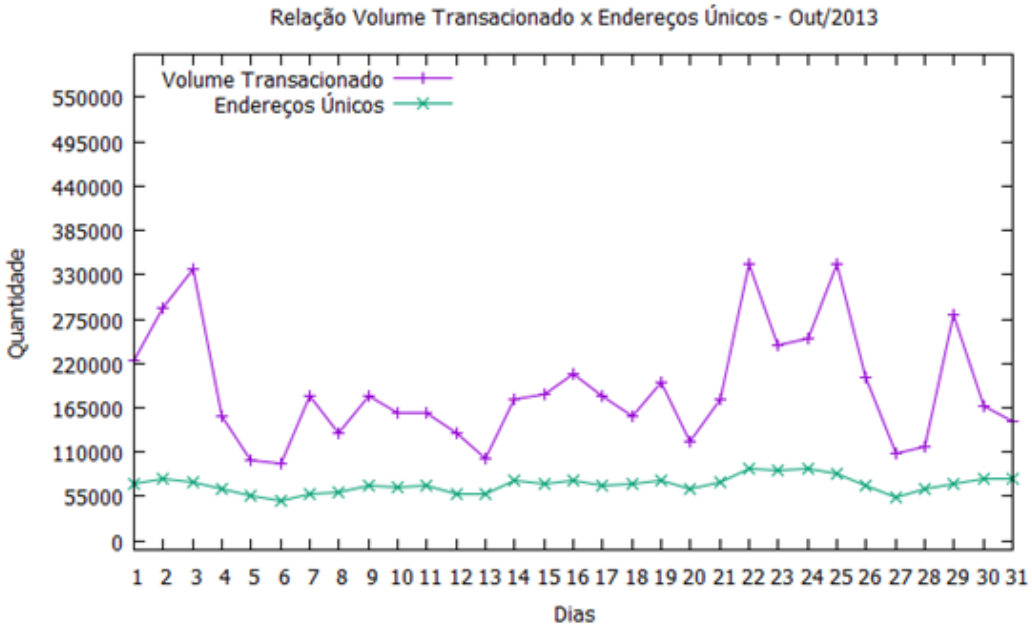

Figura 29 – Comparação entre Volume Transacionado x Endereços Únicos-Out/2013.

de endereços únicos acompanha o valor de volume transacionado. Essa característica mostra mais uma vez que usuários tendem a criar endereços novos para movimentar suas moedas. O período que compreende Outubro de 2013 e Novembro de 2013 tem grandes picos de altos valores transacionados, onde esse momento compreende os usuários movimentando suas moedas após investigações do FBI e fechamento do *Silk Road*. Já no mês de Dezembro de 2013 as altas movimentações de volumes transacionados deixam

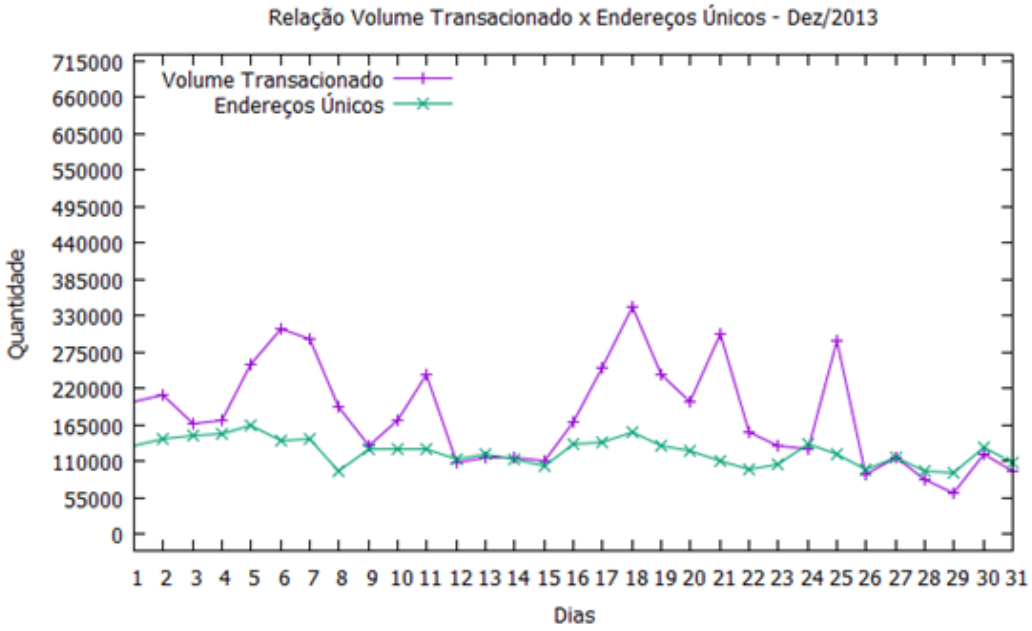

Figura 30 – Comparação entre Volume Transacionado x Endereços Únicos-Dez/2013.

de aparecer e o sistema aparenta um funcionamento normal. Com um pequeno aumento de novos usuários até mesmo para que os participantes que tinham endereços antigos e possivelmente comprometidos pela investigação do FBI comecem a utilizar novos endereços para novas negociações sem deixar rastros ou facilitar investigações e pesquisas.

6.4 Tempo de Confirmação de Blocos

O tempo de confirmação de blocos é o tempo que a rede demora para verificar e validar cada bloco antes de colocar os blocos no *blockchain*. Caso ocorra alguma tentativa de para que essa fraude possa ter sucesso essa modificação tem que ocorrer no bloco antes de ser verificado e confirmado, porque depois que o bloco foi verificado e confirmado é de extrema dificuldade desfazer uma confirmação.

Assim é mais fácil tentar alterar um bloco que não foi validado que um bloco que foi validado. A confirmação do bloco é feita através do seu *time-Stamp* e seu código *hash* que está inserido em cada bloco após sua confirmação. Essas informações são retiradas da base de dados modelada no trabalho. Na figura 31 é apresentado a tabela que contém as informações referente aos blocos do sistema Bitcoin.

A figura 31 apresenta que é possível retirar as informações de cada bloco individualmente. As informações utilizadas para calcular o tempo de confirmação de cada bloco são: a identificação do bloco e sua data e hora que foi confirmado *time stamp*. Dessa forma para conseguir o tempo que cada bloco gasta para ser confirmado basta calcular a diferença de tempo entre o último bloco e o próximo que for validado.

Figura 31 – Informação dos Blocos no Sistema Bitcoin [Spagnuolo, 2013]

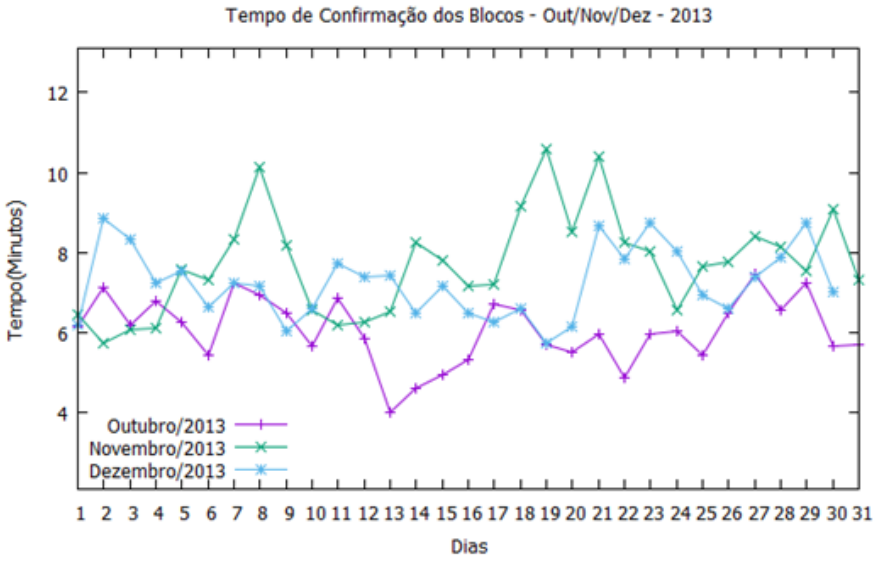

Figura 32 – Tempo de Confirmação dos Blocos

O gráfico 32 mostra a comparação dos tempos de confirmação dos blocos nos meses analisados. De acordo com [Nakamoto, 2008] o sistema deve ter um tempo médio de confirmação de 6 minutos. Entretanto o gráfico 32 apresenta algumas variações em relação ao tempo de confirmação dos blocos. Os pontos mais altos do gráfico acontecem no mês de Novembro de 2013 no momento em que a *Silk Road* sofria a investigação pelo FBI e depois seu fechamento. Vale destacar que um dos pontos faz referência ao dia 19 de Novembro esse também foi um dia no qual existem muitas transações diárias acontecendo como mostrado no gráfico 22. Desse modo o tempo que o sistema gasta para confirmar e validar novos blocos pode variar de acordo com o número de transações. Entretanto deve se levar em consideração também o número de participantes que fazem a tarefa do confirmação e validação de blocos, os chamados mineradores. Pois quanto mais mineradores mais poder computacional o sistema terá para resolver o problema *hash* dos novos blocos que precisam ser validados.

6.5 Valor de Negociação do Bitcoin

O trabalho já destacou diversos motivos que chamam a atenção de muitos usuários para a utilização do sistema. Seja para realizar transações financeiras online de forma totalmente digital e anônima ou até mesmo na tentativa de fraudar o sistema. Especificamente a tentativa de fraude tem uma relação forte com o valor da moeda bitcoin. A moeda bitcoin atualmente é obtida basicamente de três formas. A primeira dela através da compra direta de bitcoins com usuários que vendem. A segunda dela fazendo o trabalho de mineração e recebendo o pagamento em bitcoin pelo esforço realizado em criar blocos ou validar blocos. E a terceira que é através de venda comum de qualquer produto e aceitar o pagamento em bitcoin. Entretanto no meio de todas essas maneiras existe a tentativa de fraude impulsionada pelo valor significativo de mercado.

Diferente das outras variáveis que quase não são alteradas com acontecimentos externos a variável valor da moeda bitcoin é alterado fortemente por fatores externos. A cotação da moeda bitcoin funciona como uma bolsa de valores. Atualmente grandes empresas estão apostando no bitcon. Empresas como a Mastercard, IBM e até o MIT estão interessados em estudar e investir na tecnologia que o Bitcoin possui através do *blockchain*. Por esses e outros motivos a cotação sofre uma forte oscilação no seu valor negociado no mercado. O gráfico 33 apresenta o histórico de todos os valores de bitcoin já cotados. O valor de cotação como exposto anteriormente é definido por fatores externos ao sistema. Acontecimentos fora do sistema Bitcoin são os responsáveis pela definição do valor da moeda em determinado período.

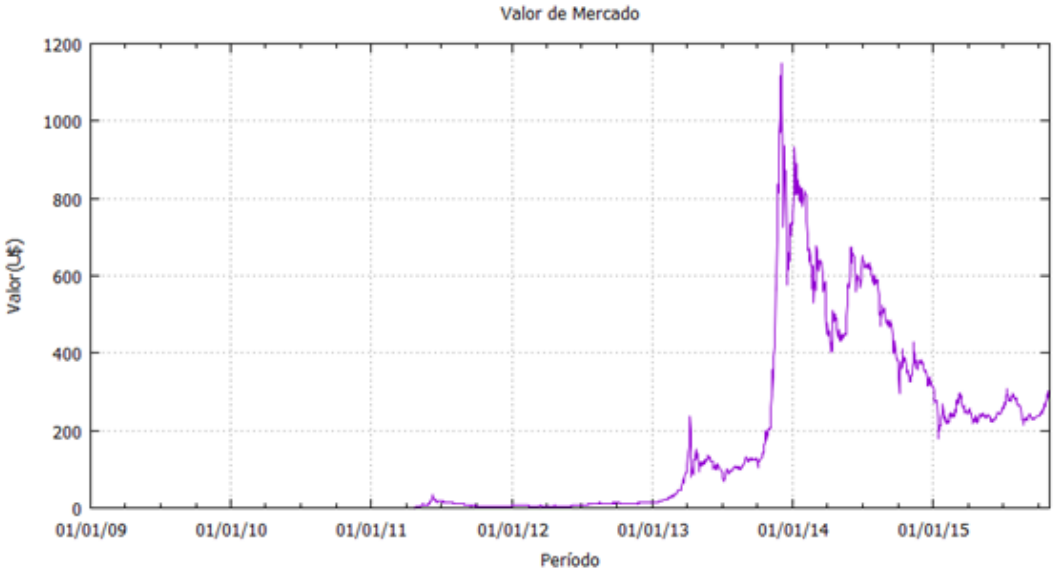

Figura 33 – Cotação da moeda bitcoin(fonte: http://www.coindesk.com/price/)

O gráfico 33 apresenta todos os valores de mercado assumidos pela moeda bitcoin

desde sua criação. Nota-se que a moeda teve uma grande valorização de 2013 a 2014 e depois entrou em desvalorização. O pico do valor de mercado da moeda bitcon acontece em Dezembro de 2014, especificamente no dia 04 de Dezembro de 2014. Esse acontecimento é o reflexo da entrada das casas de trocas de bitcoins chinesas no mercado. Nesse período a China entra no mercado Bitcoin e realiza grandes transações em volumes de bitcoins. Os volumes ultrapassavam 100 mil bitcoins dia. Entretanto logo após, o valor do bitcon sofre uma forte queda devido a noticias que a China iria bloquear a utilização de bitcoins. Paralelo a essa informação o maior site de venda e compra de bitcoins suspende todas as retiradas em bitcoin. Devido a esses fatores externos, a moeda bitcon tem seu maior valor e menor valor comprovando que fatores externos afetam sua cotação.

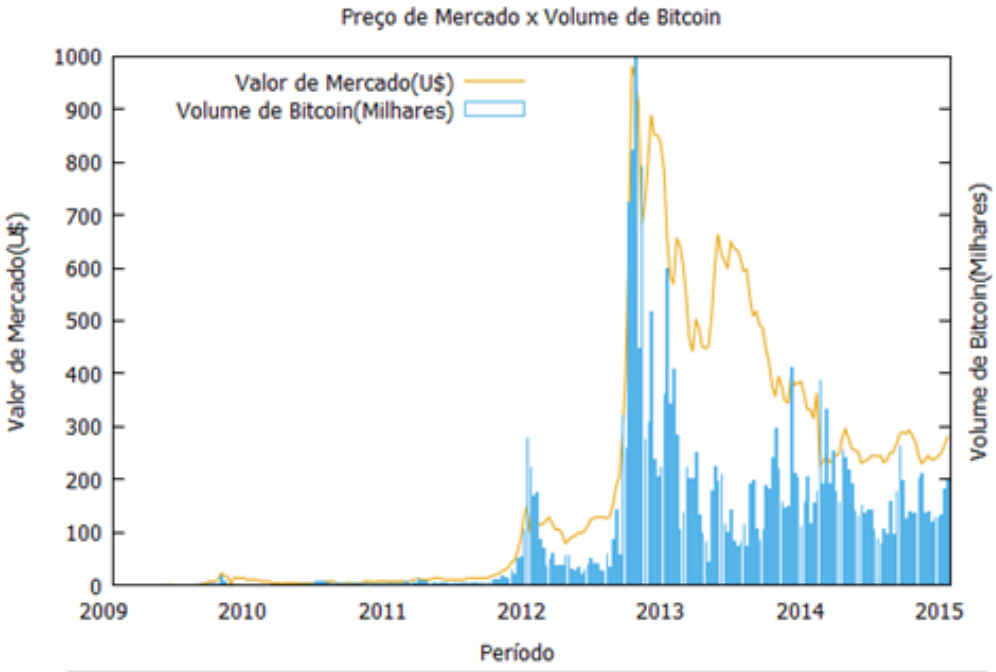

Figura 34 – Comparação Cotação x Volume de Bitcoins

Como foi apresentado, o valor de cotação da moeda bitcoin sofre com fatores externos ao funcionamento do sistema. Baseado no valor de cotação realizamos a comparação entre valor de cotação e volume transacionado. O gráfico 34 apresenta o resultado dessa comparação. O gráfico demonstra que existe uma tendência de que quando a moeda bitcoin tem um alto valor de mercado cotado a moeda é fortemente movimentada no sistema. Entretanto é apenas uma tendência, pois no período entre o ano de 2013 e 2014 o valor de mercado tinha uma cotação relativamente alta, mas o volume da moeda bitcoin transacionada não era tão alto como em outros períodos.

Apesar do pequeno período apresentado no gráfico, onde o valor de mercado é alto e o volume transacionado é baixo, em grande parte do seu funcionamento o volume da moeda bitcoin transacionada tende a ter um alto valor quando seu valor de mercado

também tem uma alta cotação. Essa característica pode ser comparada com a lei da oferta e da procura, onde existe muita procura e poucos fornecedores da moeda bitcoin, fazendo com que sua cotação aumente e tenha grande volume negociado. Esse fato ainda é acelerado devido ao crescimento do sistema e o interesse crescente de usuários interessados em comprar ou investir na moeda bitcoin.

6.6 Crescimento do Sistema Bitcoin

Através das análises individuais apresentadas nas seções anteriores do trabalho a fim de extrair características pertinentes ao funcionamento do sistema, notou-se que em grande parte as variáveis apresentam a tendência de crescimento em seus valores diários. Com a intenção de caracterizar o crescimento do sistema, o trabalho destaca duas variáveis para realizar a demonstração de crescimento do sistema desde sua criação. A análise utiliza o número total de transações e o número de endereços Bitcoins únicos utilizados. Os gráficos 35 e 36 demonstram o crescimento das variáveis confirmando o potencial e a tendência de crescimento do sistema Bitcoin.

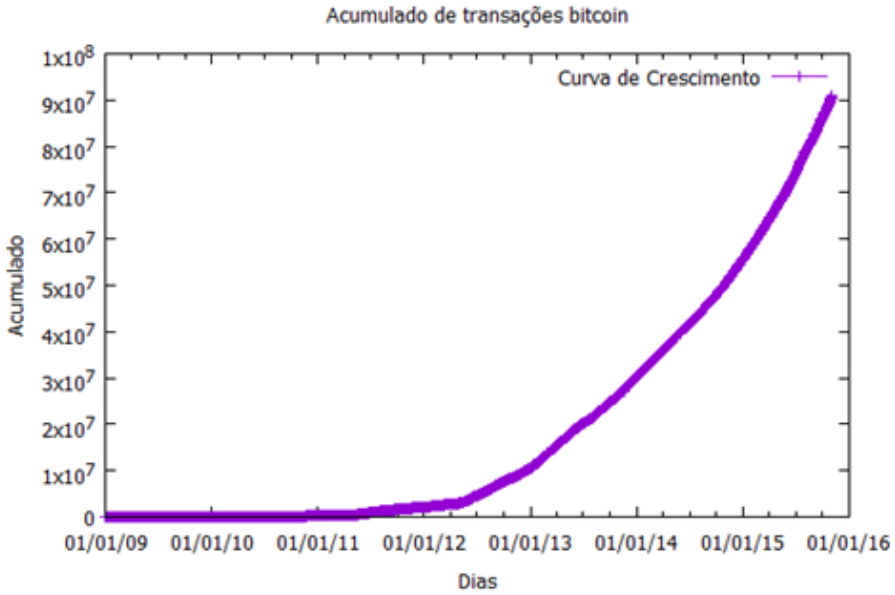

Figura 35 – Curva de Crescimento baseado no número de transações.

Os gráficos 35 e 36 demonstram uma forte tendência de crescimento do sistema Bitcoin desde sua criação. Desde a criação do sistema percebe-se que em nenhum momento o sistema teve tendência de retração. Isso demonstra que o sistema vem se tornando cada vez mais utilizado em âmbito mundial. Também confirma que devido sua confiabilidade, robustez, escalabilidade, baixo custo, anonimato e outras características vem chamando a atenção do mercado de tecnologia atual. É claro que o sistema ainda tem que passar por mais testes e estudos para confirmar ainda mais seu potencial.

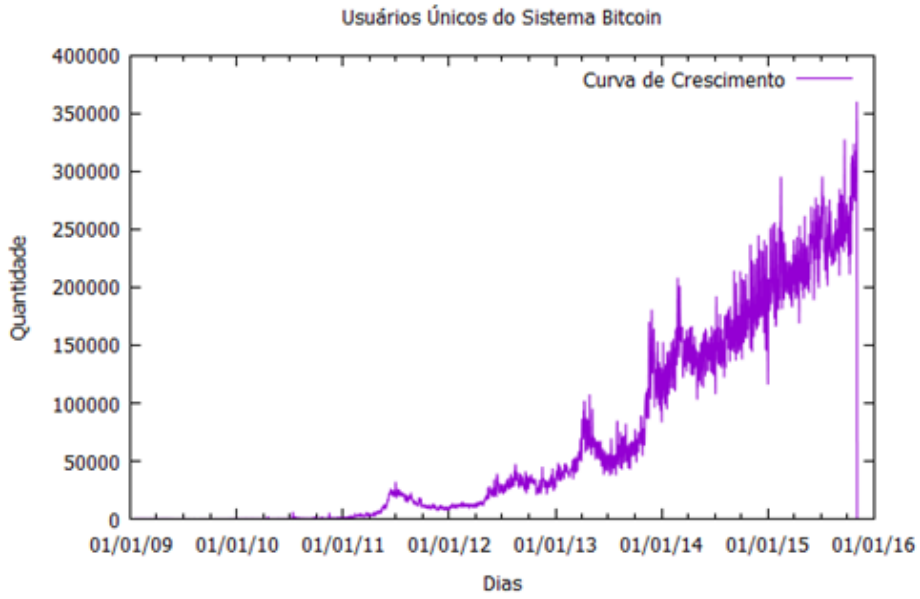

Figura 36 – Curva de Crescimento baseado no número de Usuários.

Todas as variáveis apontam crescimento do sistema Bitcoin, e tem característica positiva quando demonstra crescimento e amadurecimento do sistema. Quando o sistema tende a crescer em número de transações o *blockchain* acompanha esse crescimento. Lembrando que o *blockchain* é considerado o livro caixa de todas as transações ocorridas no sistema Bitcoin e que todo usuário participante do sistema tem uma cópia dessas informações em seu computador. Assim toda vez que o sistema cresce o *blockchain* também aumenta de tamanho. Essa preocupação é relevante porque quanto maior o *blockchain* maior o espaço ele ocupará no computador dos usuários do sistema. Esse é um ponto de estudo para evolução do sistema Bitcoin.

Até o momento a única variável que não é apontada como um valor positivo quando existe a tendência de crescimento é o tamanho do *blockchain*. Que cada vez fica maior desde sua criação e continua crescendo acompanhando o crescimento do sistema Bitcoin. O crescimento do *blockchain* esta ligado diretamente ao crescimento do número de transações demonstrado no gráfico 35. O crescimento do *blockchain* atualmente é apontado como um dos problemas do sistema Bitcoin. O crescimento impacta diretamente nos usuários do sistema principalmente nos novos usuários, que quando entram no sistema é necessário realizar a sincronização com a rede e realizar o download de todo o *blockchain* para o computador que esta entrando na rede. Por esse motivo o crescimento do *blockchain* atualmente é fonte de grandes estudos e esforços para desenvolver alguma maneira de conter seu crescimento.

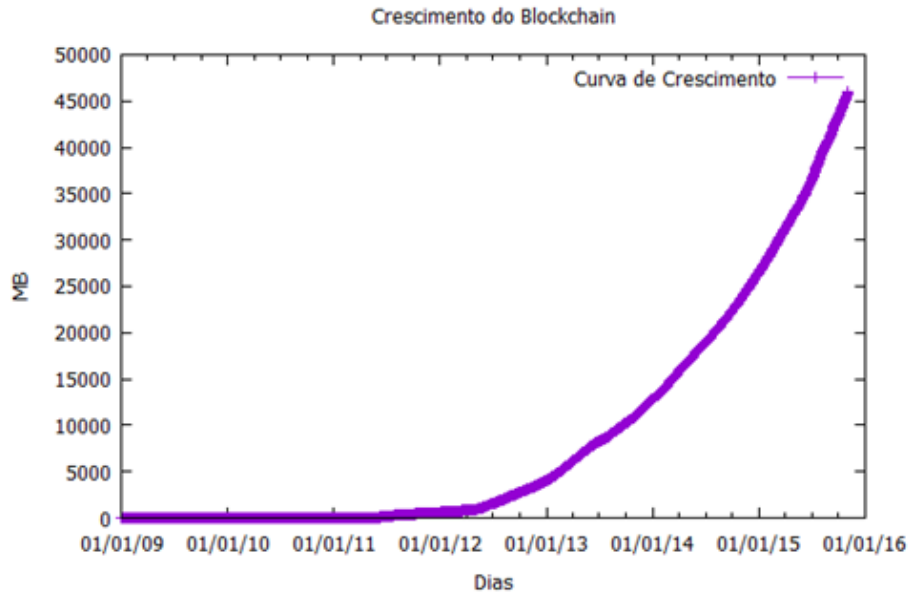

Figura 37 – Crescimento do Blockchain

7 Caracterização da Topologia da Rede Bitcoin

Esse capítulo apresenta a caracterização da estrutura da rede P2P do sistema Bitcoin. No presente trabalho destacamos a utilização da métrica de grau para identificação de usuários e da distribuição dos graus para a caracterização da estrutura do sistema Bitcoin. A métrica de grau apesar de ser uma das métricas mais simples possui grande importância na descoberta de nós que estão altamente conectados. Através da métrica de grau conseguimos determinar a importância de nós no sistema Bitcoin. Onde nós que possuem alto grau de conexão são nós que possuem uma grande influência na rede ou importância e merecem uma atenção em especial. Nos capítulos anteriores foi apresentado o estudo baseado em variáveis e caracterização da rede com informações dinâmicas do seu funcionamento diário.

De acordo com [Freeman, 1978] existem três importantes métricas de centralidade em redes complexas. Essas métricas são:grau, *closeness* e *betweenness*. [Freeman, 1978] destaca a simplicidade da métrica de grau como uma vantagem pois só a estrutura em torno do nó local precisa ser analisada e calculada para obter seu resultado. Entretanto essa métrica pode apresentar limitação de acordo com o tamanho da rede observando que a métrica de grau não leva em consideração a estrutura global. Por exemplo o nó pode estar conectado a muitos outros mas não ter uma posição na rede para requisitar, atualizar ou informar modificação rapidamente [Borgatti, 2005].

Os autores [Wehmuth e Ziviani, 2012] destacam que o conceito de centralidade é uma fonte importante para analisar redes complexas. A métrica de grau tem sua importância por ter um custo de computação baixo assim podendo ser facilmente calculada. Entretanto existem mais métricas de centralidade como /closeness] e /betweenness] mas apesar dessas métricas serem importantes possuem um alto custo de poder computacional assim as vezes inviabilizando sua utilização em experimentos.

7.1 Identificação de Usuários e Hubs no Sistema Bitcoin

Uma marcante característica do sistema Bitcoin é o anonimato de transações entre dois usuários. Entretanto utilizando o modelo de dados de análise proposto por [Espagnuolo, 2013], que esta descrito no capítulo 5 desse trabalho são gerados arquivos no formato *Pyckle* da rede Bitcoin. Esses arquivos contém informações referentes aos nós e arestas da rede do sistema Bitcoin. Para a análise desses arquivos nós criamos um *script* em *Python* para realizar a leitura dessas informações. O *script* criado nesse trabalho aplica a métrica de Grau para a identificação de usuários e classificação da estrutura do sistema Bitcoin.

7.2 Métrica de Grau para descobrir hubs e usuários importantes.

O grau de um nó em uma rede complexa é o número de arestas que incidem sobre esse nó. De acordo com [Diestel, 2005], a somatória do total de incidências sobre um determinado nó da rede define o grau do nó na rede. Também é considerado um valor que apresenta a resilência da rede onde esse valor é a capacidade da rede se manter conectada mesmo com a retirada de determinados nós.

Após as definições apresentadas no parágrafo anterior realiza-se a análise da rede Bitcoin através do *script* criado nesse trabalho para realizar o cálculo dos graus de cada nó da rede em dois determinados períodos. Os meses que são avaliados compreendem os meses de Novembro/2013 e Fevereiro/2014. O *Script* criado em *Python* utiliza a biblioteca *Networkx*. Por sua vez a biblioteca *Networkx* compreende arquivos gravados em formato *Pykle*. O *Script* percorre todos os nós de Novembro de 2013 e Fevereiro de 2014 realizando o somatório das arestas incidentes em cada nó participante do sistema no período descrito. O resultado apresenta o grau de cada nó no sistema em um determinado período.

Com o resultado é possível realizar a identificação de importantes nós da rede no sistema Bitcoin. Até mesmo identificar grandes *hubs* centralizadores de conexões. As tabelas das figuras 38 e 39 classificam os 25 nós mais importantes do sistema Bitcoin nos meses de Novembro de 2013 e Fevereiro de 2014. É interessante informar que as tabelas apresentadas no trabalho estão em forma reduzida, pois as análises ocorreram por todo o período de Novembro de 2013 e Fevereiro de 2014. Isso compreende um número muito superior de nós em cada mês. A tabela 5 apresenta a quantidade de nós da rede nos dois períodos.

Mês	**Número de Nós**
Novembro/2013	999.427
Fevereiro/2014	1.048.575

Tabela 5 – Número de Nós analisados nos dois períodos

Com uma melhor análise nas tabelas 6 e 7 dos dois meses é possível extrair duas características interessantes que são exibidas quando é analisada a rede completa durante um mês. As características destacam que nos dois meses existe uma grande quantidade de nós com apenas uma conexão ou grau 1 e uma outra pequena parcela de nós sem conexão ou grau 0.

Mês	**Número de Nós sem Grau**
Novembro/2013	1.480
Fevereiro/2014	1.862

Tabela 6 – Número de Nós sem Grau nos dois períodos

Nó	Endereço	Grau
node	1LuckyG4tMMZf64j6ea7JhCz7sDpk6vdcS	28396
node	14cZMQk89mRYQkDEj8Rn25AnGoBi5H6uer	23389
node	1cointQVgw2EwnJx3EFVPvD65gSsD9nJ7	23007
node	1dice97ECuByXAvqXpaYzSaQuPVvrtmz6	17717
node	1DXst9N2J5zrrurdKqqoEjfZ7BBAAESjtH	17576
node	1Bet32kBtZzXViMs1PQHninHs4LADhCwtB	12267
node	1AqTMY7kmHZxBuLUR5wJjPFUvqGs23sesr	10624
node	1KFHE7w8BhaENAswwryaoccDb6qcT6DbYY	9740
node	16xFkvuKaVGZQw9ECA1u124P665kVroxgS	9131
node	1dice9wcMu5hLF4g81u8nioL5mmSHTApw	7572
node	1LuckyY9fRzcJre7aou7ZhWVXktxjjBb9S	7445
node	1969VR2qCchXMW94tpcYirbVLUfFw4Pw7b	6989
node	1dice8EMZmqKvrGE4Qc9bUFf9PX3xaYDp	6834
node	1LuckyR1fFHEsXYyx5QK4UFzv3PEAepPMK	6418
node	1changemCPo732F6oYUyhbyGtFcNVjprq	6037
node	1MSFDdeDJF4DqsPgPSM8zxZroe17CLP6RK	4912
node	1278USLSVEgbm9NKjjD3ukt9him5pjnbHi	4798
node	1Cwb33nqn4S2uDsXwhNrUNy7FPdiRYhyM8	4765
node	1Bet16kGTPwHKEbvNK4uQKtYC61Q4MHBst	4549
node	19M8T7DNCqGxtq1JytB8q2Krs5hWmsakNn	4490
node	1Bet2yV8rPt7kE14AAbhYnxqw53uhCQd7T	4313
node	1Gemk2fKb3hvgs4bi3hW3y8vCaJJrx42NC	4139
node	15ZY5nbr2SLtAP22La7323uTBEsM9XxfTZ	4128
node	19PkHafEN18mquJ9ChwZt5YEFoCdPP5vYB	3888
node	1MH1cNAbjpZAGE1CVJksbuXXSptSYJF1us	3737

Figura 38 – Grau dos 25 nós mais importantes no mês de Novembro/2013

A tabela 6 representa a quantidade de nós que não possuem grau nenhum na rede P2P do sistema Bitcoin. Essa quantidade de nós não representa nem 0,5% do número de nós que possuem grau na rede Bitcoin no período analisado. Lembrando que todos nós que possuem ao menos 1 grau, indica que esse nó já realizou alguma transação na rede Bitcoin.

Mês	**Número de Nós com Grau 1**
Novembro/2013	123.875
Fevereiro/2014	82.092

Tabela 7 – Número de Nós Com Grau 1

A segunda característica revela que uma grande quantidade de nós pertencentes à rede Bitcoin só realizam uma única transação. Por esse motivo apresentam grau 1. Essa característica tende a comprovar que muitos usuários criam novos endereços para realizar transações únicas com intuito de dificultar o rastreamento de transações. No mês de Novembro de 2013 a quantidade de nós com grau 1 representa um pouco mais de 12%

Nó	Endereço	Grau
node	1KFHE7w8BhaENAswwryaoccDb6qcT6DbYY	133817
node	1CjPR7Z5ZSyWk6WtXvSFgkptmpoi4UM9BC	42513
node	1Facb8QnikfPUoo8WVFnyai3e1Hcov9y8T	39383
node	1Ne5bGjDdgmbsGdNK9ocwrQiWf8K1FTuSa	38768
node	1cointQVgw2EwnJx3EFVPvD65gSsD9nJ7	31688
node	13p4zncq6m3Ax7tvKhEG2k49hgwfS5g7ic	22313
node	1CGVyAgAx9gg1va5pGNVJtF6gdKpPUVTSf	21477
node	1NyCoyWBhZxZ4EqbWBSNDiSwt76PtzK1Zm	19842
node	1LuckyY9fRzcJre7aou7ZhWVXktxjjBb9S	19163
node	1bones5gF1HJeiexQus6UtvhU4EUD4qfj	15751
node	1Mf478S7eWk7SmjJ7XmUX1c65mWFCqCkFK	14862
node	1JiixnNK52kMtxMRuC26YMsyCxoBZzkinw	13525
node	1dice8EMZmqKvrGE4Qc9bUFf9PX3xaYDp	12843
node	1bonesEeTcABPjLzAb1VkFgySY6Zqu3sX	12635
node	1Kqnt8DnZxFcM9NrfzdHDdKFGWQdynq4Q3	11177
node	1Fvz8iTnSUZXWdFNmiFXunrwoqdZzKRT2E	10527
node	1E84FvZUPvMRrXdvDHkB3uCgPYtLJmu9r8	10378
node	1PqXxCDX2CCZXTrbLKBrr3fWPumh8ZdjpJ	9772
node	1bones2wX8sqGHcuXeKPzHgZegtL2dnGC	9772
node	1bones8VWK2LbDYZ8TJAME9gpHaV2ZCGT	8343
node	18ozftq32S4ppV5tPLtg7Eb12GJt8j2B34	7459
node	1RCodeej35kS9rGMG7HsbZmB4U8n6mg7D	7205
node	1ChANGeATMH8dFnj39wGTjfjudUtLspzXr	7205
node	1HsbRerjd4bNMpds6ewQ7XY24oSx4zg5fs	7095
node	15WtLXz24WitRWtfdEzWPWZJYYDEBjjhUf	6839

Figura 39 – Grau dos 25 nós mais importantes no mês de Fevereiro/2014

do número de nós da rede. Em comparação com o mês de Fevereiro de 2014 em que o número de nós com graus 1 diminuiu e representou um pouco menos de 8% de nós da rede. Ainda com o agravante de que no mês de Fevereiro de 2014 o número de nós da rede foi extremamente grande como apresentado na tabela 5. O motivo de um número maior de nós com grau 1 em novembro de 2013 tem uma forte relação com o fechamento da *Silk Road* que ocorreu no mesmo período. Desse modo em Novembro de 2013 muitos usuários tenderam a criar novos endereços para realizar movimentação de moedas bitcoin e dificultar o rastreamento das transações.

7.3 Identificando usuários

Como apresentado na seção anterior após a análise do resultado gerado pelo *script* criado no trabalho, é possível visualizar o endereço de cada nó participante no sistema Bitcoin e qual o seu grau. Partindo desse ponto conseguimos identificar quais endereços

são importantes ou possuem um alto grau na rede. Como o sistema tem a premissa do anonimato entre transações não conseguimos identificar quem são os usuários através do endereço. Entretanto de forma bem simples é possível a descoberta de quem são os responsáveis pelos endereços. Nesse trabalho após identificarmos quem são os usuários com maior grau na rede, pegamos o endereço Bitcoin descoberto como apresentado na tabela 39 e fizemos uma busca na Internet através do site `www.google.com` e iniciamos uma pesquisa e investigação. Logo após algumas buscas conseguimos facilmente a identificação de quem é o responsável pelo endereço Bitcoin. O primeiro endereço pesquisado foi:1KFHE7w8BhaENAswwryaoccDb6qcT6DbYY.

Esse endereço no mês de Fevereiro de 2014 foi o endereço com maior grau da rede naquele período com 133.817 conexões. As figuras 40 e 41 apresentam o resultado da pesquisa realizada na Internet afim de descobrir quem é o responsável pelo endereço Bitcoin.

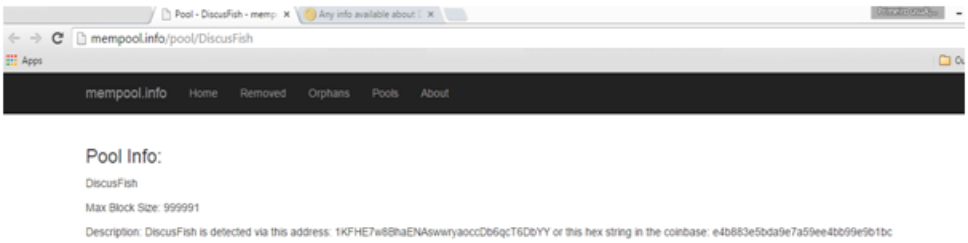

Figura 40 – Identificando usuários 1.

Figura 41 – Identificando usuários 2.

Realizando um novo teste com o endereço 1LuckyG4tMMZf64j6ea7JhCz7sDpk6vdcS com maior grau agora no período de Novembro de 2013. O endereço teve 28.396 conexões no mês de Novembro de 2013, sendo o endereço da rede naquele período com o maior grau. As figuras 42 e 43 mostram o resultado da segunda pesquisa no novo endereço.

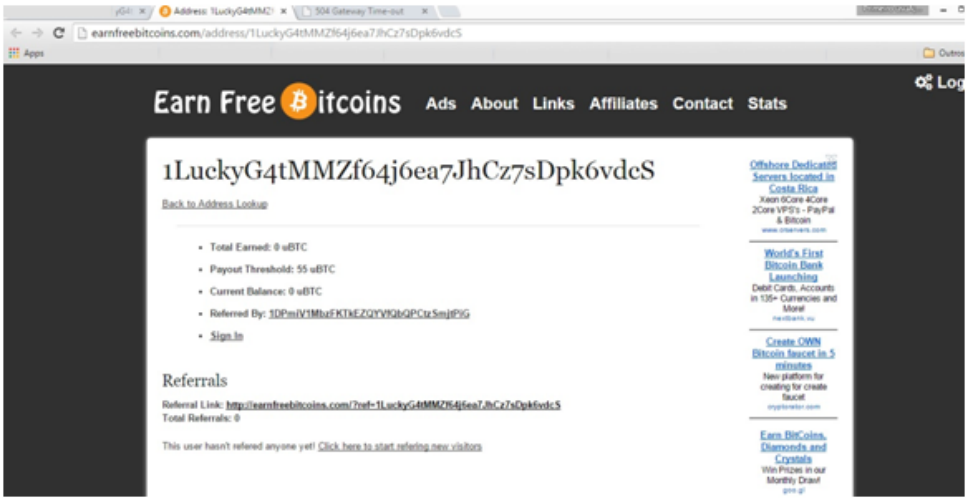

Figura 42 – Identificando usuários 3.

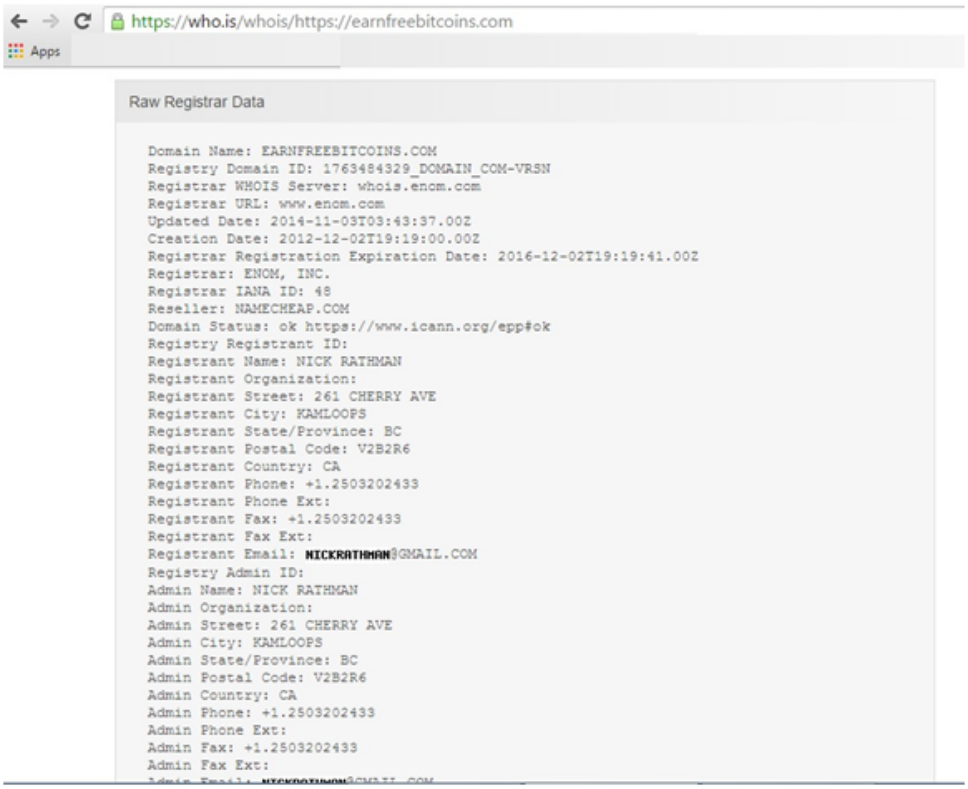

Figura 43 – Identificando usuários 4.

Dessa forma conseguimos descobrir quem são os responsáveis pelos endereços Bitcoins pequisados. Claramente a rede do sistema Bitcoin já não possui a característica total de anonimato como podemos ver nos casos analisados acima. Nos dois testes foi possível descobrir quem são os responsáveis pelos endereços Bitcoin. É claro que essa forma de descoberta é trabalhosa e requer as vezes uma investigação maior e demorada. Em alguns casos a pesquisa certamente não irá nos retornar quem é o responsável pelo endereço Bitcoin utilizado.

Dessa maneira o trabalho mostra que é possível identificar usuários no sistema Bitcoin, seja realizando a descoberta pelo endereço mais importante levando em consideração o grau do endereço ou realizando a pesquisa pelo endereço na Internet e apontando seu responsável por aquele endereço. Mas a rede ainda continua tendo um forte anonimato entre transações, bastando que os usuários criem endereços novos. Entretanto grandes lojas que passam a aceitar Bitcoin não vão realizar a troca de seu endereço tão facilmente, pois isso pode acarretar um grande problema de comunicação com seus clientes ou usuários que realizam transações. Desse modo a rede Bitcoin claramente perde um pouco do seu anonimato entre os usuários.

7.4 Caracterização da Estrutura da Rede Baseada na Distribuição de Grau.

No capítulo 2 do trabalho são apresentadas as três principais estruturas de redes complexas. Essas estruturas compreendem-se nos seguintes modelos: redes aleatórias, redes pequeno-mundo, e redes livre de escala. Analisando a rede P2P do sistema Bitcoin é possível classificar sua estrutura. Para obter essa classificação partimos da distribuição do grau da rede. O trabalho analisou os meses de Novembro de 2013 e Fevereiro de 2014. Os gráficos 44 e 45 mostram uma tendência de classificação da sua estrutura.

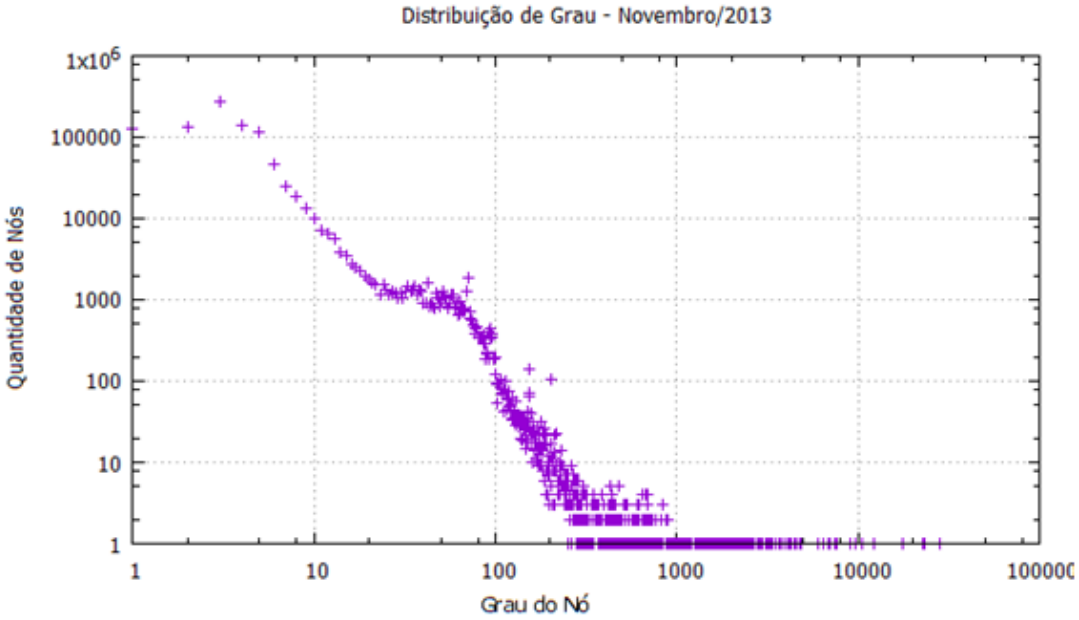

Figura 44 – Distribuição de Grau-Novembro/2013

Os gráficos 44 e 45 apresentam muita semelhança em relação a sua distribuição de grau dos nós da rede. Realizando a comparação com o modelo proposto por [Barabási e

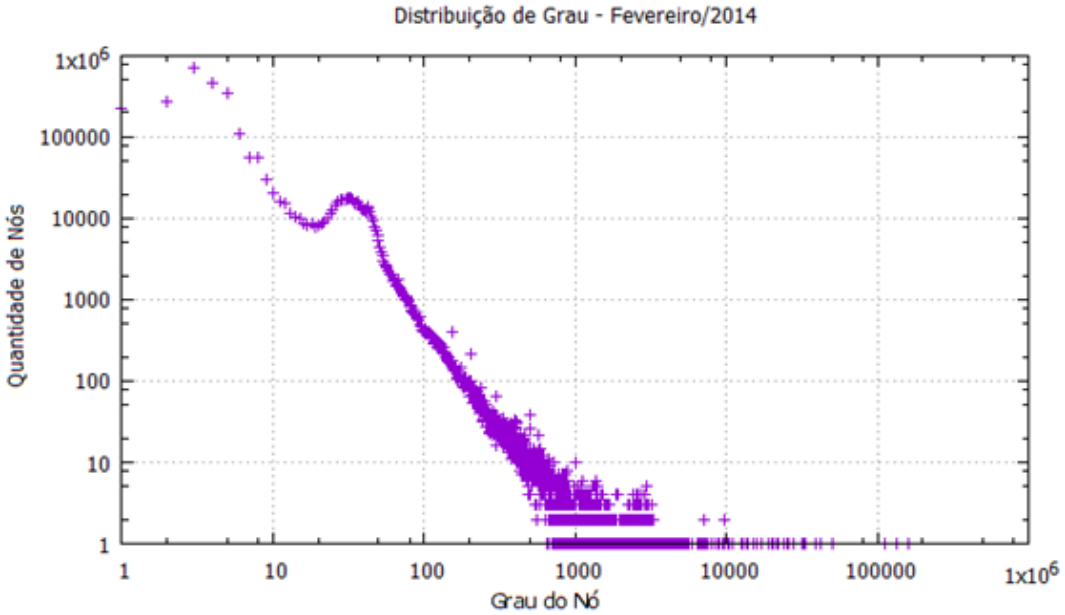

Figura 45 – Distribuição de Grau-Fevereiro/2014

Albert, 1997], é possível classificar a rede P2P do sistema Bitcoin como uma rede Livre de Escala. A figura 5 deste trabalho apresenta a semelhança entre os gráficos 44 e 45 e o modelo proposto por [Barabási e Albert, 1997]. O modelo proposto por [Barabási e Albert, 1997], segue a tendência de uma distribuição de grau seguindo a lei da potência. Também é fácil observar nos gráficos 44 e 45 que a rede P2P do sistema Bitcoin possui poucos nós altamente conectados e muitos nós pouco conectados. Essa característica é outro fator que é apresentado nos gráficos 44 e 45. Assim mais uma vez classificando a rede do sistema Bitcoin de forma que tende a uma rede livre de escala. Através da caracterização de sua estrutura o sistema Bitcoin passa a ser analisado de acordo com uma rede livre de escala que possui diversas características importantes em relação a sua composição. No capítulo 2 deste trabalho foi apresentado características e detalhes importantes a respeito da redes Livres de Escala.

8 Considerações Finais

Apesar do sistema Bitcoin ser uma nova tecnologia muitos pesquisadores se interessaram pelo seu estudo pois o sistema tem um potencial inovador, revolucionário e robusto capaz de se tornar um meio de realizar transações financeiras totalmente digital descentralizada. Podemos perceber que ainda temos poucos trabalhos na área mas já temos bons trabalhos que tratam do assunto. Atualmente a importância do tema se mostra bastante forte quando o MIT cria um laboratório de pesquisa voltado totalmente para o estudo dos sistemas de criptomoedas, o laboratório denominado *Digital Currency Initiative*. O laboratório conta com um dos principais desenvolvedores do protocolo Bitcoin, Gavin Andresen. O laboratório tem como seu principal ponto de pesquisa as questões de segurança, estabilidade, escalabilidade, privacidade e economia.

Esse trabalho teve como objetivo apresentar os principais conceitos do sistema Bitcoin e suas características de dinamicidade em relação a variáveis do seu funcionamento diário. Apresentamos como realizar a extração dos dados do *blockchain* para estudo dos mesmos. E por fim fizemos um estudo da dinamicidade do sistema Bitcoin baseado nos resultados retirados do *blockchain* e seus valores mensais e diários.

Entretanto o sistema ainda tem muito a ser estudado. Questões como segurança, estabilidade não foram tratadas nesse trabalho e devem ser muito exploradas ainda. Também destacamos que através dos meios de extração de dados aqui apresentados é possível criar estudo em relação a estrutura da rede P2P que da suporte ao sistema Bitcoin. Como trabalhos futuros é interessante criar um framework facilitando toda a modelagem de dados do sistema bitcoin e até mesmo criar um classificador de endereços bitcoins. Outra proposta é aprofundar em estudos para propor uma solução ou melhoria do crescimento do tamanho do blockchain do sistema Bitcoin, que atualmente tem um crescimento continuo.

Por fim apesar de algumas restrições o sistema Bitcon se mostra um sistema com forte tendencia revolucionária e apresenta um grande crescimento desde sua criação. Esse crescimento apresentado aqui no presente trabalho. Atualmente o sistema está em evidência e a todo momento é destaque nos assuntos que estão relacionados a novas tecnologias e economia. Certamente o sistema Bitcoin merece atenção nos próximos anos.

REFERÊNCIAS

[Adroutsellis-Theotokis e Spinellis, 2004] Stephanos Androutsellis-Theotokis and Diomidis Spinellis. A survey of peer-to-peer content distribution technologies. ACM Computing Surveys, 36(4):335-371, December 2004. (doi:10.1145/1041680.1041681)

[Alex Hern, 2013] Alex Hern. Bitcoin: what you need to know. Available online, 2013. URL http://www.theguardian.com/technology/2013/oct/04/ bitcoin-what-you-need-to-know-silk-road.

[Alex Hern, 2013] Alex Hern. Bitcoin price surges to post-crash high. Available online, 2013. URL http://www.theguardian.com/technology/2013/oct/21/ bitcoin-price-surges-to-post-crash-high.

[Balakrishnan, 2003] BALAKRISHNAN, H., KAASHOEK, M. F., KARGER, D., MORRIS, R., STOICA, I. Looking Up Data in P2P Systems. MIT Laboratory for Computer Science.

[Barabási e Albert, 1997] A.-L. Barabási and R. Albert. Emergence of scaling in random networks. Science, 286:509-512, 1997.

[Barabási e Albert, 1999] Barabsi, A. L. and Albert, R. (1999a). Emergence of scaling in random networks. Science, pages 286-509.

[Barabási, 2003] Barabási, A. L. (2003). Linked: How everything is connected to everything else and what it means for business, science and everyday life. Plume.

[Borgatti, 2005] Borgatti, S.P. (2005). Centrality and network flow. Soc. Networks, 27, 55?71.

[Buchanan, 2002] Buchanan, M. (2002). Nexus - small world and the groundbreaking science of network. W. W. Norton Company.

[Brugere, 2012] Ivan Brugere. Anomaly detection in the Bitcoin transaction network. Technical report, ESP-IGERT, 2012.

[Diestel, 2005] Diestel, R. Graph Theory, volume 173 de Graduate Texts in Mathematics.Third. ed., Springer-Verlag, Heidelberg, 2005.

[D. Ron and A. Shamir, 2013] D. Ron and A. Shamir. Quantitative Analysis of the Full Bitcoin Transaction Graph. In Proceedings of Financial Cryptography 2013.

[Elli Androulaki, 2013] Elli Androulaki, GhassanO. Karame, Marc Roeschlin, Tobias Scherer, and Srdjan Capkun. Evaluating user privacy in Bitcoin. In Ahmad-Reza Sadeghi, editor, Financial Cryptography and Data Security, volume 7859 of LNCS, pages 34-51. Springer, 2013.

[F.Reid e M. Harrigan, 2011] F. Reid and M. Harrigan, An analysis of anonymity in the Bitcoin system, in Privacy, security, risk and trust (PASSAT), 2011 IEEE Third Internatiojn Conference on Social Computing (SOCIALCOM). IEEE, 2011, pp. 1318-1326.

[Freeman, 1978] Freeman, L. C., 1978. Centrality in social networks: Conceptual clarification. Social Networks 1, 215-239.

[Jerry Britto e Andrea Castillo, 2013] Jerry Brito and Andrea Castillo (2013). "Bitcoin: A Primer for Policymakers".Mercatus Center. George Mason University. Retrieved 26 Junho 2015.

[Joshua Kopstein, 2013] Joshua Kopstein (12 December 2013). "The Mission to Decentralize the Internet". The New Yorker. The networks "nodes-users running the bitcoin software on their computers-collectively check the integrity of other nodes to ensure that no one spends the same coins twice. All transactions are published on a shared public ledger, called the "block chain"

[Kashmir Hill, 2013] Kashmir Hill. Five reasons for Bitcoins most recent price surge. Available online, 2013. URL http://www.forbes.com/sites/kashmirhill/2013/10/23/five-possible-reasons-for-bitcoins-most-recent-surge/

[Lugin e Yong, 2015] Luqin Wang and Yong Liu. Exploring Miner Evolution in Bitcoin Network. Passive and Active Measurements (PAM) Conference, March 2015(PAM-15).

[Jean Metz, 2007] Metz, Jean; Calvo, Rodrigo; Seno, Eloize; Romero, Roseli; Liang,

Zhao; ?Redes complexas: conceitos e aplicações?, Universidade de São Paulo, Janeiro de 2007.

[Nakamoto, 2008] Bitcoin: A Peer-to-Peer Electronic Cash System, unpublished manuscript, retrieved at http://pdos.csail.mit.edu/6.824/papers/bitcoin.pdf - Nakamoto - 2008.

[Newman, 2003] Newman, M. (2003). The structure and function of complex networks. volume 45, pages 167-256. SIAM Review

[P.Erdos e A. Rényi, 1959] P. Erdos and A. Rényi. On random graphs. Publicationes Mathematicae, 6:290-297, 1959.

[Ratnasamy, 2001] RATNASAMY, S.; FRANCIS, P.; HANDLEY, M.; KARP, R.; SHENKER, S. A Scalable Content-Addressable Network. ACM SIGCOMM 2001.

[Rowstron, 2001] ROWSTRON, A.; DRUSCHEL, P. Pastry: Scalable, distributed object locationand routing for large-scale peer-to-peer systems. In Proc. 18th IFIP/ACM International Conference on Distributed Systems Platforms (Middleware), Heidelberg, Germany, pages 329-350.

[Sarah Meiklejohn, 2013], Sarah Meiklejohn, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M Voelker, and Stefan Savage. A fistful of bitcoins: characterizing payments among men with no names. In Proceedings of the 2013 Internet Measurement Conference, pages 127-140. ACM, 2013.

[Spagnuolo, 2013] Michele Spagnuolo. BitIodine: Extracting Intelligence from the Bitcoin Network. PhD thesis, Politecnico di Milano, 2013.

[Stanley Milgran, 1967] S. Milgran. The small world problem. Psychology Today, 1(1):60-67, 1967.

[Stoica, 2001] STOICA, I.; MORRIS, R.; KARGER, D. R.; KAASHOCK, M; DABEK, F.;BALAKRISHNAN, H. Chord: A scalable peer-to-peer lookup protocol for internet applications. In Proceedings of the ACM SIGCOMM, pages 149-160, San Diego, California.

[Stribling, 2004] STRIBLING, J.; RHEA, S.; JOSEPH, A.; KUBIATOWICZ, J. Tapestry: A Resilient Global-scale Overlay for Service Deployment, IEEE Journal on Selected Areas in Communications.

[Strogatz, 2001] Strogatz, S. H. (2001). Exploring complex networks. Nature, 410:268-276. http://dx.doi.org/10.1038/35065725.

[Watts e Strogatz, 1998] Watts, D. J. and Strogatz, S. H. (1998). Colletive dynamics of small-world networks. Nature, (393):440-442.

[Wehmuth e Ziviani, 2012] Wehmuth, K., Ziviani, A.: Distributed assessment of the closeness centrality ranking in complex networks. In: SIMPLEX, NY, USA (2012).