UNIVERSIDADE FEDERAL FLUMINENSE
INSTITUTO DE COMPUTAÇÃO
BACHARELADO EM SISTEMAS DE INFORMAÇÃO

ALISSON PESSANHA QUINTANILHA

O USO DE BITCOINS COLORIDAS COMO UMA MOEDA COMPLEMENTAR VIRTUAL: UMA ANÁLISE DE VIABILIDADE

Niterói
2016

ALISSON PESSANHA QUINTANILHA

O USO DE BITCOINS COLORIDAS COMO UMA MOEDA COMPLEMENTAR VIRTUAL: UMA ANÁLISE DE VIABILIDADE

Trabalho de conclusão de curso apresentado ao curso de Bacharelado em Sistemas de Informação, como requisito parcial para conclusão do curso.

Orientador:
Prof. Dr. Leonardo Cruz da Costa.

Coorientador:
Prof. Me. Luiz Arthur Silva de Faria.

Niterói
2016

ALISSON PESSANHA QUINTANILHA

O USO DE BITCOINS COLORIDAS COMO UMA MOEDA COMPLEMENTAR VIRTUAL: UMA ANÁLISE DE VIABILIDADE

Trabalho de conclusão de curso apresentado ao curso de Bacharelado em Sistemas de Informação, como requisito parcial para conclusão do curso.

Aprovado em 04 de Abril de 2016.

BANCA EXAMINADORA

Prof. Dr. Leonardo Cruz da Costa (Orientador) – IC/UFF

Prof. Me. Luiz Arthur Silva de Faria (Coorientador) – HCTE/UFRJ

Prof.ª Dra. Isabel Leite Cafezeiro – IC/UFF

Prof. Dr. Ilaim Costa Júnior – IC/UFF

Niterói
2016

Ficha Catalográfica elaborada pela Biblioteca da Escola de Engenharia e Instituto de Computação da UFF

Q7 Quintanilha, Alisson Pessanha
O uso de bitcoins coloridas como uma moeda complementar virtual: uma análise de viabilidade / Alisson Pessanha Quintanilha. – Niterói, RJ : [s.n.], 2016.
105 f.

Trabalho (Conclusão de Curso) – Departamento de Sistemas de Informação, Universidade Federal Fluminense, 2016.
Orientadores: Leonardo Cruz da Costa, Luiz Arthur Silva de Faria.

1. Tecnologia computacional. 2. Bitcoins. 3. Economia solidária. 4. Moeda social. I. Título.

CDD 004

A todos os estudantes de baixa renda que não se deixam esmorecer pelas adversidades socioeconômicas do nosso pequeno mundo.

AGRADECIMENTOS

Em ordem alfabética, aos professores Isabel Leite Cafezeiro, Leonardo Cruz da Costa, Luiz Valter Brand Gomes e Rosângela Lopes Lima, os quais foram para mim um referencial de pensamento crítico, questionador, pensamento que busca entender a complexidade, e não simplificar de forma ilusória a realidade. Também os agradeço pelo empenho dedicado ao curso de Sistemas de Informação da Universidade Federal Fluminense, pela coragem de questionar, de propor mudanças, de buscar evolução. Não tenho dúvidas de que o curso de graduação em Sistemas de Informação da UFF tem evoluído de forma muito benéfica graças ao trabalho de professores dedicados como vocês.

We can only see a short distance ahead, but we can see plenty there that needs to be done.

Alan Turing

RESUMO

O surgimento de iniciativas e movimentos de caráter econômico alternativo dentro do sistema capitalista, ao quais são ao mesmo tempo capazes de destruir e de reconstruir as relações de troca e os padrões de consumo típicos de tal sistema capitalista, levou ao surgimento de novas tecnologias computacionais, bem como conduziu ao surgimento de novos casos de uso para as tecnologias existentes. Dentre essas tecnologias computacionais emergentes, o Bitcoin se destaca como tecnologia candidata a ser moeda neutra, independente de quaisquer autoridades governamental ou bancária, criando novos casos de uso para a troca de bens e serviços a partir de uma quebra de paradigmas de produção e de controle daquilo que a sociedade tipicamente considera moeda. Um desses novos casos de uso seria a criação de moedas privadas, de escopo local, comunitário, a partir das *colored bitcoins*. Entretanto, a aplicação de tais tecnologias computacionais e sua relação com os esquemas de organização social que produzem moedas próprias (moedas sociais, locais, comunitárias e complementares), os quais precedem ao surgimento de tal tecnologia, figura de forma extremamente omissa na literatura existente. Este trabalho irá analisar a viabilidade de se usar o protocolo Bitcoin, por meio do complemento arquitetural conhecido como *colored bitcoins*, no contexto de moedas sociais, locais, comunitárias e complementares, as quais, neste trabalho, viremos a chamar apenas de complementares. Em teoria, as *colored bitcoins* seriam capazes de fazer as vezes de meio circulante nos sistemas de moedas complementares. Entretanto, embora isto seja assim sugerido pela comunidade gestora do Bitcoin, concluímos que entre seus membros atuantes não há um perfeito entendimento dos modos de organização e das necessidades de tais sistemas de moedas complementares. Nossas conclusões apontam para a impossibilidade de se utilizar as *colored bitcoins* como equivalente perfeito ao papel-moeda ou ao dinheiro eletrônico no contexto de sistemas de moedas complementares. Concluímos, ainda, que a adoção de tal tecnologia computacional implicaria em diversas limitações e vulnerabilidades técnicas, jurídicas e econômicas, restringindo sua aplicabilidade, na prática, a um cenário experimental.

Palavras-chave: Moedas locais. Moedas comunitárias. Moedas sociais. Moedas complementares. Protocolo Bitcoin. *Colored bitcoins.* Bitcoins coloridas.

ABSTRACT

The emergence of initiatives and movements proposing alternative economic settings within Capitalism, which at the same time disrupt and rebuild trading relationships and patterns of consumption characteristics of such system, leads to the emergence of new computing technologies, as well as to the emergence of new use cases for existing technologies. Among such emergent technologies, Bitcoin stands out as an aspirant currency, being independent of governmental and banking authorities, defining new use cases for the trading of goods and services, breaking the paradigm of what society typically considers money, as well as the ways of emitting and controlling a currency. One of such new use cases is the creation of private currencies, at a local or community setting, by using colored bitcoins. However, the harnessing of such computing technologies and its application within social environments in the form of a currency scheme (social, local, community or complementary currencies) is loosely described in the literature. The present work will analyze the viability of using Bitcoin protocol, through its architectural complement called colored bitcoins, as a form of local, social, community or complementary currency, which in this work we will be referring to exclusively as complementary currencies. In theory, colored bitcoins can operate as money in the same way as a complementary currency does. However, even though Bitcoin community suggests such use case, we conclude that there is not enough understanding among active Bitcoin community members regarding the needs and organizational processes of a complementary currency scheme. Our conclusions point that it would not be possible to use colored bitcoins as a perfect match for paper money or electronic cash in the context of a complementary currency. We also conclude that the adoption of such computing technology would bring several limitations of technical, legal and economic order to such schemes, thus restricting its usage to an experimental setting.

Keywords: Local currencies. Community currencies. Social currencies. Complementary currencies. Bitcoin protocol. *Colored bitcoins.*

LISTA DE ILUSTRAÇÕES

Figura 1 – Block chain (visão externa da arquitetura do Bitcoin) 65
Figura 2 – Encadeamento de transações (visão interna da arquitetura do Bitcoin) 70

LISTA DE TABELAS

Tabela 1 – Características Gerais dos Sistemas de Moedas Complementares 49
Tabela 2 – Vulnerabilidades nos Sistemas de Moedas Complementares 51
Tabela 3 – Comparação dos Sistemas de Moedas Complementares Identificados Previamente com o Cenário de Adoção das Bitcoins Coloridas 86
Tabela 4 – Comparação das Vulnerabilidades Identificadas Previamente nos Sistemas de Moedas Complementares com o Cenário de Adoção das Bitcoins Coloridas 89

LISTA DE ABREVIATURAS E SIGLAS

BNDES	Banco Nacional de Desenvolvimento Econômico e Social
BCDs	Bancos Comunitários de Desenvolvimento
BTC	bitcoin
CC	*Community Currency*
CC	*Complementary Currency*
CLCs	*Convertible Local Currencies*
LETS	L*ocal Exchange Trading Systems*
MB	*Megabyte* (ou 1024 *bytes*)
MMORPGs	*Massively Multiplayer Online Role-Playing Games*
PNAD	Pesquisa Nacional por Amostra de Domicílios
USD	*United States dollar*

SUMÁRIO

1 INTRODUÇÃO 15

2 REVISÃO DA LITERATURA 23

2.1 O CONCEITO DE MOEDA 23

2.1.1 O Que É Moeda? 23

2.1.2 Moeda Política, Moeda Econômica e Moeda Social. 25

2.1.3 Moedas Complementares 26

2.1.4 Moedas Criptográficas 31

2.2 MOEDAS CRIPTOGRÁFICAS COMO MOEDAS COMPLEMENTARES 35

3 MOEDAS COMPLEMENTARES COMPARADAS 38

3.1 DEFINIÇÃO DAS CLASSES DE MOEDAS COMPLEMENTARES 38

3.2 COMPARAÇÃO DAS CLASSES DE MOEDAS COMPLEMENTARES 48

4 O PROTOCOLO BITCOIN E AS BITCOINS COLORIDAS 52

4.1 O PROTOCOLO BITCOIN 53

4.1.1 Origem do Bitcoin 53

4.1.2 Funcionamento do Bitcoin 55

4.2 BITCOINS COLORIDAS 71

5 BITCOINS COLORIDAS COMO UMA MOEDA COMPLEMENTAR 76

5.1 ASPECTOS TÉCNICOS 76

5.2 ASPECTOS JURÍDICO-ECONÔMICOS 79

5.3 CARACTERÍSTICAS COMPARADAS 82

6 CONSIDERAÇÕES FINAIS 90

REFERÊNCIAS 94

GLOSSÁRIO 100

1 INTRODUÇÃO

Quando o laureado com o Nobel da Paz, Muhammad Yunus, inaugurava o Grameen Bank em 1983, abria-se o caminho para que novos modelos de negócios surgissem dentro do sistema capitalista. Negócios esses que substituíam o foco no lucro individual pelo foco na resolução de um problema coletivo, seja o problema de se reduzir o desperdício, seja o de se aproveitar melhor os recursos ou ferramentas ociosas, seja o de acabar com a pobreza extrema em uma determinada região. Conforme definido por Grove & Berg (2014), o negócios sociais visam aplicar os métodos e práticas dos negócios tradicionais - os quais visam ao lucro - para alcançar uma mudança social. Tal conceito pode, na superfície, parecer idêntico ao que o terceiro setor representa no Brasil, mas há diferenças significantes em sua origem e em seus princípios.

O terceiro setor brasileiro - o qual passou a ter garantia jurídica de sua existência com o Código Civil em 1916 - é caracterizado por ser "não governamental" e "não lucrativo" (SILVA, 2010). Nisso sua semelhança é bastante grande com os negócios sociais, que, como mencionado anteriormente, são iniciativas privadas que não visam ao lucro individual, mas sim à resolução de um problema social. A diferença entre ambos, entretanto, se dá em termos de princípios e métodos empregados. O terceiro setor brasileiro guarda forte relação com os movimentos eclesiais, de origem alicerçada nos princípios da filantropia e da caridade religiosa (SILVA, 2010), enquanto os negócios sociais tem por alicerce os princípios empresariais. Conforme exposto por Grove & Berg (2014), o modelo Grameen, que é o modelo estabelecido por Yunus para negócios sociais, envolve sete princípios, dentre os quais – para fins de tornar evidente a diferença entre os negócios sociais e o terceiro setor – destacamos: "ser financeiramente e economicamente sustentável" e "o investidor recebe de volta apenas o valor investido".

Há que se notar aqui que a palavra "apenas" indica que o investidor poderia, ou deveria, ter expectativas de receber algo mais em troca do valor investido, visto que se trata de um negócio e não de caridade. Entretanto, em um negócio social o único dividendo devido ao investidor é a mudança social em si (GROVE e BERG, 2014). Portanto, o lucro do investidor é a mudança social patrocinada por ele. Não se trata apenas de um lucro psicológico, no sentido de que esse investidor teria satisfação interna por estar transformando a realidade, mas sim de um lucro real que o beneficiará indiretamente por reduzir problemas sociais ou ambientais da comunidade - em sentido estrito ou amplo - em que esse investidor está inserido. O investidor financia um negócio social tendo em vista as mudanças sociais que ele deseja ver no mundo e, por princípio,

paga-se de volta ao investidor o valor investido, pois um negócio social deve ser autossustentável. Esse, entretanto, não é um princípio do terceiro setor, onde é comum a doação de recursos não reembolsáveis a entidades sociais. Uma evidencia deste fato é que o BNDES – o qual segundo o Art. 3º do Decreto nº 4.418, de 11 de Outubro de 2002 é um "instrumento de execução da política de investimento do Governo Federal" – possui uma linha de crédito dedicada a investimentos não-reembolsáveis, os quais foram estabelecidos pelo Decreto-Lei nº 1.940, de 25 de Maio de 1982 no seu artigo 6º, que confere ao BNDES a responsabilidade de administrar o Fundo de Investimento Social (FINSOCIAL). Tal linha de investimentos é destinada justamente a iniciativas de caráter eminentemente assistencial, como as de entidades do terceiro setor.

Yunus (2010), de forma bastante pragmática, considera que o passo mais importante para se lançar um negócio social é "ter uma ideia promissora". Entretanto, como ele mesmo explica, para que uma ideia seja capaz de se transformar em um negócio social, ou seja, para que essa ideia resolva um problema social de forma duradoura, é necessário que esta seja autossustentável e que seja capaz de "delegar poderes" (do inglês, *empower*) aos envolvidos – o que significa não reduzir ou até mesmo aumentar sua autodeterminação e autonomia –. Ainda de acordo com o economista, ainda que essa ideia necessite refinamentos e posterior desenvolvimento, se ela possui as supracitadas características, é possível que o idealizador já tenha tudo que é necessário para se aventurar no mundo dos negócios sociais (YUNUS, 2010). A ideia original de Yunus que resultou no Grameen Bank foi criar um sistema de microcrédito sustentado por um sistema de confiança pessoal. Tal ideia surgiu a partir da constatação de que pequenas quantias de dinheiro, da ordem de centavos de dólar, eram impeditivos para que trabalhadores pobres de Bangladesh pudessem operar seus negócios. Havia ainda o agravante de que as taxas de juros cobradas pelos agiotas sobre tais valores ínfimos eram extremamente altas, da ordem de 10% por semana e vinham acompanhadas da imposição de vender toda a produção para o próprio agiota a preços ditados por eles mesmos, traduzindo-se, na prática, em uma forma de escravidão (YUNUS, 2010). Em seu livro, Grove & Berg (2014) trazem vários estudos de caso de negócios sociais, oriundos de diferentes países, que vão desde um sistema de crédito a estudantes pobres ao uso dos sistemas de informação para transformar a realidade de agricultores. Uma evidencia de que o movimento dos negócios sociais tem prosperado e se mantém relevante é o fato de que o nome Grameen se tornou uma alcunha para uma família de organizações, para além do banco de microcrédito criado por Yunus. Dentre essas organizações, a Grameen Intel Social Business Ltd. (GISB) desenvolve aplicativos móveis para ajudar na

redução da mortalidade infantil e na melhoria da eficiência de lavouras. Esses projetos tiram proveito do fato de que mesmo famílias pobres naquela região frequentemente possuem um aparelho móvel no qual o aplicativo pode ser instalado.

A popularização do telefone celular abriu espaço para que outras iniciativas comerciais visando a colaboração pudessem surgir e prosperar no sistema capitalista. No Brasil, de acordo com a Pesquisa Nacional por Amostra de Domicílios mais recente feita pelo IBGE (PNAD 2013, tabela 7.7), 90% dos domicílios com renda familiar de até 10 salários mínimos tinham pelo menos um telefone celular. Dentre as iniciativas que fazem uso intenso do aparelho celular como plataforma, destaca-se o movimento conhecido como Consumo Colaborativo (do inglês *Collaborative Consumption*, às vezes também chamado de *sharing economy*, peer economy, collaborative economy ou on-demand economy, que podem ser traduzidos respectivamente como economia da partilha, economia dos pares, economia colaborativa e economia sob demanda, respectivamente, embora todos esses termos possuam especificidades que lhe conferem significados próprios distintos). Esse movimento une a agilidade e a versatilidade das redes *peer-to-peer* (P2P) com o poder computacional de fácil acesso - por meio do computador pessoal e, posteriormente, por meio dos aparelhos celulares - para criar negócios onde antes, sem a existência dessas tecnologias, não seria possível ou seria inviável economicamente. O termo Collaborative Consumption (CC) é adotado por Botsman (2015) para descrever esse movimento, sendo na visão da autora o termo de escopo mais amplo para definir essa economia que, ao mesmo tempo em que é parte do sistema capitalista, busca reinventar o consumo tradicional por meio da tecnologia, eliminando intermediários nas trocas entre indivíduos, rompendo com os padrões de consumo vigentes e se tornando um antagonista do consumismo e do aproveitamento precário de recursos (BOTSMAN, 2015). Botsman é uma pesquisadora da economia colaborativa e coautora do livro *What's Mine Is Yours: The Rise of Collaborative Consumption* (O Que É Meu É Seu: A Ascenção do Consumo Colaborativo, em tradução nossa). Em seu artigo publicado na seção Co.Exist da página da Internet da revista Fast Company a autora define cada um dos jargões usados para se referir ao consumo colaborativo, os quais são frequentemente usados de forma intercambiável, causando confusão. Como não é necessário ao escopo deste trabalho, deixaremos a critério do leitor o aprofundamento nessas definições, caso julgue relevante. Para fins de qualquer menção futura neste trabalho, iremos adotar consumo colaborativo como o único termo para se referir a esses movimentos de reinvenção das relações econômicas entre indivíduos por meio do emprego da tecnologia computacional.

O cerne do consumo colaborativo está em tirar vantagem das tecnologias de comunicação e informação (TIC) para organizar a partilha de recursos, ou para melhor aproveitar esses recursos. A maior semelhança entre a economia colaborativa e os negócios sociais reside no fato de que a determinação de se resolver um problema deve estar no cerne da iniciativa empreendedora, notavelmente um problema que envolva o sub aproveitamento de recursos, tais como um bem material, uma ferramenta ou um espaço privado (BOTSMAN, 2015). Entretanto, as tecnologias de informação e comunicação, como a Internet, telefones celulares e *softwares* aplicativos são recursos essenciais para que se estabeleça uma economia colaborativa, são esses recursos que permitem coordenar a oferta e a demanda de forma economicamente viável, pois de outra forma seria extremamente custoso organizar a dinâmica de uma economia que permita, por exemplo, o uso alternado de recursos ociosos. Outro fator de extrema importância, tanto nos negócios sociais quanto no consumo colaborativo, é a confiança entre os indivíduos participantes.

O problema da confiança é recorrente em sistemas de informação descentralizados, e a construção de confiança em serviços remotos, sejam serviços B2C ou C2C pode ser obtida de diversas formas, a depender das necessidades específicas daquele serviço em especial. Quanto mais descentralizada for a administração de um serviço, e quanto maior o número de participantes envolvidos, mais difícil se torna operá-lo de forma eficaz sem que haja um bom sistema de confiança. Por exemplo, só é possível ter alguma confiança nos artigos da Wikipedia porque existe uma instituição mantenedora criada pelos fundadores, a Wikimedia, a qual hospeda o *website* e controla as diretrizes do sistema de revisão por pares. Logo, cria-se um sistema de reputação em que apenas indivíduos confiáveis podem participar. Botsman considera que um sistema de reputação como esse é um elemento chave para economias colaborativas, elevando a confiança ao nível de "moeda" dessa nova economia (BOTSMAN, 2012).

Uma outra solução para o problema da confiança, que ao mesmo tempo resolve um problema de interesse social, é o reCAPTCHA. A sigla CAPTCHA significa "Completely Automated Public Turing Test to tell Computers and Humans Apart", o que nada mais é que um teste de Turing completamente automatizado, ou seja, uma forma totalmente programável, automatizada, de se realizar um teste de Turing para determinar se a interação em uma dada página *web* tem como origem um ser humano ou um programa de computador (um robô, uma rotina automatizada). O reCAPTCHA, é um teste de Turing que utiliza uma palavra que não pode ser reconhecida por um computador como pergunta a ser respondida pelo interlocutor supostamente humano (AHN, MAURER, *et al.*, 2008). Dentre as críticas ao reCAPTCHA, a

mais pertinente diz respeito ao fato de que o trabalho de digitalização de documentos, obtido como produto da resposta dada por um ser humano, é realizado de forma alienada, ou seja, a grande maioria dos participantes não sabe que estão contribuindo para a digitalização de documentos. Isso poderia, inclusive, ser considerado algo intencional no projeto do reCAPTCHA, o que é pode ser visto como má fé, como um uso indevido do trabalho alheio para colher uma vantagem particular. De fato, os arquivos do jornal The New York Times, datados a partir de 1851, foram digitalizados por meio do reCAPTCHA, em um projeto patrocinado pela Google chamado Google Books Project. Entretanto, tais documentos não estão disponíveis para consulta gratuita, estando disponíveis apenas para os assinantes do serviço. Portanto, o reCAPTCHA certamente seria um exemplo de um uso inteligente dos sistemas de informação para se resolver o problema da confiança, porém não pode ser considerado uma solução verdadeiramente colaborativa ou social.

Um outro requisito fundamental para que se opere uma economia que envolva colaboração entre os pares é o custo de se realizar transações, especialmente quando se deseja realizar pagamentos de baixo valor agregado, ou micro pagamentos. Dado que a colaboração surge como um elemento inovador e, ao mesmo, destruidor da economia capitalista, podem surgir dificuldades ao se tentar adaptar os recursos e processos vigentes, surgidos na economia capitalista tradicional, a esses novos modelos. Um desses problemas é justamente o uso de cartões de crédito como meio de pagamento em transações de pequenos valores, pois as taxas cobradas por transação podem ser altas demais para que se opere micro pagamentos. Isso aconteceu com o próprio Muhammad Yunus, que precisou criar seu próprio banco, o Grameen, dadas as dificuldades encontradas por ele ao tentar operar os microcréditos por meio de um banco tradicional indiano (YUNUS, 2010).

Um estudo publicado pelo IEEEXpress em 2007 já apontava o uso de criptografia como uma solução mais difícil, porém de longo termo, para se resolver o problema dos micro pagamentos, problema este que seria uma das principais barreiras limitadoras da então florescente economia baseada em uso de aparelhos móveis, na qual se inclui o consumo colaborativo. As vantagens do uso de criptografia estariam em determinadas características dessa abordagem, tal como a capacidade de se agregar transações independentes para fins de processamento por meio de uma cadeia de *hash* (TRIPUNITARA e MESSERGES, 2007). Coincidência ou não, pouco tempo depois, em 2009, o Bitcoin surgiu discretamente na Internet como uma tecnologia que se propunha a ser uma moeda criptográfica, tendo como base de funcionamento o uso de

assinaturas digitais e de cadeias de *hash*. O Bitcoin se lançava como sendo ao mesmo tempo moeda e um meio de pagamento independente de instituições bancárias, na prática independente de qualquer entidade terceira. Portanto, o Bitcoin não só inaugurava o uso das moedas baseadas em criptografia, como também rompia o paradigma vigente, sendo uma tecnologia totalmente independente de qualquer instituição gestora, confiando o poder de validação de todas as transações exclusivamente a uma rede P2P descentralizada, ou seja, aos usuários do Bitcoin. Portanto, o Bitcoin resumia em si tanto a questão da confiança plena nos participantes do sistema, quanto a solução para o problema dos micro pagamentos, podendo ser considerado uma iniciativa eminentemente comunitária.

Várias moedas virtuais surgiram após o Bitcoin, algumas alcançando maior notoriedade que outras, mas nenhuma evoluiu tanto, ou se tornou tão popular ou tão estudada quanto a precursora. Dentre as moedas alternativas de maior uso no momento da escrita deste trabalho, as duas mais importantes, em termos de valor de mercado, são o Bitcoin e o Litecoin. O Bitcoin foi a primeira moeda virtual e é ainda a que tem apresentado maior evolução, como o surgimento de inovações incrementais, que utilizam a estrutura do Bitcoin para novos casos de uso, algo que não existe nas demais moedas virtuais. Em 2012, o matemático israelense Meni Rosenfeld estabeleceu as bases para que se usasse o protocolo Bitcoin como arcabouço para outras espécies de transações, tornando possível a realização de outros registros relevantes, que não simplesmente pagamentos sobre a infraestrutura do Bitcoin. Dentre esses novos casos de uso propostos, se encontra a criação de moedas locais. O cerne dessa inovação proposta por Rosenfeld está na introdução da capacidade de se "colorir" moedas virtuais, permitindo, assim, que se possa utilizar a estrutura do protocolo Bitcoin para transferência de propriedade de bens digitais, para a emissão de ações, de vales promocionais ou até mesmo para a criação de moedas privadas, locais (ROSENFELD, 2012). Entretanto, há ainda poucos estudos que analisem o potencial das moedas criptográficas como uma tecnologia componente de economias comunitárias, locais ou colaborativas. Além disso, há pouquíssimos registros de instituições ou associações que tenham utilizado o protocolo Bitcoin para tal finalidade. Logo, alguns questionamentos pertinentes surgem: O que é exatamente uma moeda local, moeda social, moeda comunitária ou moeda complementar? Seria o Bitcoin, enquanto tecnologia surgida em um dado contexto, para uma dada finalidade, realmente compatível com o que são as moedas locais, comunitárias, sociais, alternativas, complementares? Como eu faria para criar uma moeda local com escopo de atuação dentro de uma universidade? Onde está a documentação

completa e a descrição dos casos de uso das *colored bitcoins*? Diante de tamanha omissão, seria realmente possível usar essa tecnologia para criar uma moeda local?

O objetivo do presente trabalho é compreender o que são e quais são os tipos de moedas alternativas existentes, especialmente aquilo que se costumam chamar de moedas locais, sociais, comunitárias e complementares na literatura. Além disso, temos como objetivo compreender o funcionamento do Bitcoin, especificamente das *colored* bitcoins, analisando até que ponto esta tecnologia pode efetivamente funcionar como componente chave, ou seja, como moeda, como dinheiro eletrônico, como meio de troca, na infraestrutura de uma moeda dita local, comunitária, social ou complementar. Como hipóteses consideramos que o uso dessa tecnologia teria o potencial de trazer benefícios para os sistemas de moedas comunitárias, tais como: a) a capacidade de eliminar a necessidade de se ter uma gerência responsável pela coordenação da mecânica de funcionamento de tais moedas; b) substituir a emissão de papel-moeda, tornando mais barato e mais fácil o processo de criação de uma moeda; c) substituir o uso de cartões de crédito, eliminando, assim, as taxas cobradas por suas operadoras e a necessidade de se alugar máquinas de processamento de pagamento (*point of sale machines*).

Como objetivos específicos temos: a) Identificar as principais características das moedas ditas locais, sociais, comunitárias ou complementares; b) Criar um sistema de classificação, definindo classes ou modelos capazes de agrupar as diferentes experiências relatadas na literatura; c) Descrever o funcionamento do Bitcoin enquanto tecnologia, expondo as motivações de seu surgimento, a teoria que a embasa, os componentes chave que a sustentam, as pessoas envolvidas na sua manutenção, os custos decorrentes do seu uso e a confiança técnica que se pode ter nela. d) Explicar como as *colored bitcoins* são implementadas tendo por base a infraestrutura do protocolo Bitcoin; e) Identificar as potencialidades e as fraquezas do uso das *colored bitcoins* como moeda, analisando seu nível de compatibilidade com cada classe definida previamente, especialmente em termos técnicos e jurídico-econômicos.

Na seção 2 deste trabalho, dedicada à revisão da literatura, serão apresentados e definidos os principais conceitos necessários à compreensão deste trabalho, bem como serão apresentados os trabalhos correlatos. A seção 3 irá identificar os sistemas de moedas sociais, locais, comunitárias e complementares existentes e classifica-los para fins de análise de compatibilidade das *colored bitcoins* com tais sistemas de moedas. Tal análise se encontra na seção 5. Na seção 4 explicamos em profundidade os componentes chave do protocolo Bitcoin,

a fim de chegarmos à compreensão do que são as *colored bitcoins* e de como são implementadas. Esse conhecimento é necessário para uma maior compreensão das implicações da adoção do Bitcoin nos sistemas de moedas. Por fim, na seção 6, tecemos considerações finais e apresentamos algumas sugestões de trabalhos futuros.

2 REVISÃO DA LITERATURA

A fim de se analisar os possíveis usos do Bitcoin enquanto moeda complementar, é necessário investigar primeiramente quais são as categorias de moedas alternativas existentes. Como as moedas ditas locais, comunitárias ou sociais (as quais serão, a seguir, agrupadas sob o termo "moedas complementares") se distinguem das demais? Como tais moedas surgiram e quais são suas características principais? É necessário também, identificar o que são moedas criptográficas e quais usos (ou aplicações) para tais moedas encontram embasamento na literatura. Este capítulo se dedicará a elucidar tais questões, bem como apresentará os principais conceitos relevantes para o escopo deste trabalho na visão de diferentes autores. Cabe ressaltar, ainda, que neste capítulo elegeremos termos de referência a serem usados nos demais capítulos deste trabalho sempre que houver sobreposição ou divergência conceitual entre termos na literatura, como ocorre com os termos moeda local, moeda social, moeda comunitária e moeda complementar. Por fim, apresentaremos os principais trabalhos correlatos que vieram a propor usos para as moedas criptográficas, sobretudo no contexto de moedas complementares.

2.1 O Conceito de Moeda

2.1.1 O Que É Moeda?

Não pretendemos nesta seção fazer uma análise aprofundada do conceito de moeda, mas sim tornar clara a definição do que é moeda a partir da visão de diferentes autores. Serão brevemente explorados aspectos jurídicos, econômicos, antropológicos e sociais do que é moeda, sendo que o viés social permite uma interpretação um tanto não convencional do conceito de moeda e não está presente no trabalho de todos os autores citados.

Para Freire (2011), em uma primeira concepção – possivelmente a concepção mais imediata – moeda refere-se, em sentido estrito, apenas à moeda metálica ou ao dinheiro (papel moeda), a qual é de emissão exclusiva da autoridade monetária. Para Caminha & Figueiredo (2011), entretanto, moeda é gênero, da qual dinheiro é espécie. Nessa concepção moeda pode ser qualquer bem que viabilize permutas, enquanto o dinheiro seria o bem eleito pelo Estado. Porém, Freire (2011), também defende que o conceito de moeda – em sentido estrito – é frequentemente bem mais amplo, não havendo consenso entre autores, especialmente entre estudiosos de diferentes campos do saber. Tal conceito pode abarcar facilmente diferentes meios de pagamento, inclusive aqueles com respaldo no direito contratual privado, como ativos financeiros, títulos, obrigações bancárias, ou a qualquer *commodity* (FREIRE, 2011).

Em uma concepção jurídica, o conceito de moeda só faz sentido quando amparado por um conjunto de normas que lhe asseguram a existência, a exigibilidade e, portanto, o próprio valor, pois de outra forma os pagamentos ou promessas de pagamento seriam apenas "palavras ao vento". Grau (1995 apud Freira, 2011) defende que as definições postas pelo direito positivo são imprescindíveis para que a moeda possa exercer suas funções, quais sejam: a) a definição de qual medida será adotada como unidade de conta, isto é, como referencial para preços; b) a definição de qual o padrão de valor, como, por exemplo, o padrão-ouro, no qual toda moeda deveria estar lastreado em ouro; c) a definição de quais instrumentos possuem poder liberatório, ou seja, poder de eximir o devedor de suas obrigações jurídicas. Sob um ponto de vista econômico, entretanto, a definição de moeda se baseia exclusivamente nas funções que ela exerce. Assim, qualquer coisa pode ser considerada moeda, desde que exerça as seguintes funções: funciona como meio de troca; funciona como padrão de valor e funciona como um estoque de riqueza (FREIRE, 2011). Nessa concepção, uma moeda sem lastro em metais é perfeitamente válida, haja vista que esse é o caso de todas as moedas emitidas pelos Estados Soberanos na atualidade. É importante, ainda, ressaltar que tais moedas emitidas pelos Estados possuem como características o curso legal e o curso forçado. O curso legal refere-se ao fato de que tal moeda não pode ser rejeitada como meio de pagamento, já o curso forçado refere-se à inconversibilidade de tal moeda, ou seja, não só tais moedas não são lastreadas em metais, como é proibida a conversão da moeda em seu lastro, seja ele um lastro real, de existência material, ou não (CAMINHA e FIGUEIREDO, 2011).

Uma análise antropológica apontará para a moeda como sendo um bem estimado por um grupo social, o qual é eleito como meio dinamizador das trocas. A necessidade de se eleger um bem como meio de troca adviria do desequilíbrio natural entre a oferta de certos bens e a escassez de outros, o que impossibilitaria a troca direta. O valor de tal bem frequentemente reside em sua utilidade, por exemplo, o sal, mas tal utilidade pode ter origem em sua apreciação estética ou subjetiva, por exemplo, conchinhas de pequenos crustáceos (CAMINHA e FIGUEIREDO, 2011). Entretanto, conforme enfatizado por Mishkin (2000 apud FREIRE, 2011), para que uma mercadoria possa ser eleita como moeda, ela deve atender a determinados requisitos, tais como: ser de fácil padronização, ser de ampla aceitação, ser divisível, ser de fácil transporte e ser durável. O entendimento da importância de cada um desses requisitos é intuitivo: a padronização visa prevenir fraudes e facilitar a determinação do valor da moeda; a ampla aceitação é imperativa para que um – e apenas um – bem possa ser eleito como moeda; a divisibilidade é necessária para que "o troco" possa existir; a facilidade de transporte é óbvia,

pois seria inviável realizar trocas sem que se pudesse facilmente transportar a moeda de um lugar para o outro e, por fim, a durabilidade diz respeito à não deterioração do bem, o qual, como já vimos, deve servir como estoque de riqueza. De nada adiantaria se ter uma moeda que perca o seu valor de forma irreversível, especialmente se a deterioração desse valor for extremamente rápida ou abrupta.

Por fim, em uma visão sociológica, moeda pode ser conceitualmente considerada como um meio de comunicação entre indivíduos. Nessa concepção, a moeda pode ter como funções: estabelecer coesão entre um determinado grupo de indivíduos; transformar a organização social desse grupo ou preservar as relações existentes; ou ainda, proteger esse grupo contra ameaças externas (VOLKMANN, 2012). Essa definição de moeda é especialmente útil como um arcabouço para se pensar o papel das moedas ditas regionais ou sociais, as quais não servem meramente a funções monetárias, mas sevem prioritariamente a funções sociais. Essa definição também encontra algum paralelo com a afirmação de Botsman (2012), de que a confiança é uma moeda no consumo colaborativo, já que a medida da reputação de um determinado indivíduo é algo aceito por todos os participantes como tendo valor em tais sistemas, bem como é um meio de comunicar algo aos participantes e mantê-los coesos, mantê-los participando daquele sistema de transações. Entretanto, a medida da confiança individual presente em tais sistemas não cumpre qualquer outra função de moeda discutidas nesta seção, logo confiança não pode ser considerada moeda quaisquer outros efeitos que não a alusão ao seu valor para o indivíduo em tais sistemas.

2.1.2 Moeda Política, Moeda Econômica e Moeda Social.

Moeda política pode ser definida como a moeda emitida pelo Estado Nacional, ou pela autoridade política local, a qual possui curso legal. Incluem-se nessa categoria moedas emitidas por províncias, comunidades ou mesmo moedas emitidas por territórios separatistas. Por outro lado, moeda econômica seria a moeda emitida por uma empresa, visando ao lucro. Podem ser incluídas nessa categoria as moedas bancárias, sob a forma de depósitos ou dívidas bancárias. No caso dos bancos, essa moeda geralmente coincide com a moeda de curso legal. Outros exemplos de moeda econômica seriam vale-compras ou vale-presentes e pontos de programas de fidelização de clientes (FREIRE, 2011).

Freire (2011) defende que as moedas sociais não se enquadram totalmente em nenhuma dessas duas categorias gerais de classificação de moedas, mas podem ser um híbrido. São moedas

emitidas por instituições formais ou informais, representativas dos interesses de uma determinada comunidade. Tais moedas estão em seu cerne caracterizadas pela solidariedade, pelo estreitamento dos laços entre os componentes do grupo social que as utilizam e o desenvolvimento econômico local. Porém, como ressalta a autora, essa fronteira entre as categorias de moedas é discutível.

O conceito de moeda social é largamente empregado na literatura brasileira para se referir a esta forma de economia solidária. Pode-se inferir que essa escolha busca enfatizar o aspecto social da atividade, no sentido de que esta iniciativa – de se criar uma moeda – tem como aspecto principal o exercício de um papel de relevância social. Papel social este que frequentemente se assemelha ao papel exercido por movimentos de cunho assistencial do terceiro setor brasileiro, o que frequentemente resulta na equiparações de tais movimentos para fins de descrição dos mesmos na literatura, tornando difícil a identificação do surgimento da economia solidária no Brasil (CAMINHA e FIGUEIREDO, 2011). Vale frisar, que tal equiparação é errônea, visto que a economia solidária produz um visível desenvolvimento econômico e, em termos de força política transformadora, poderiam ser considerada como uma evolução das economias sociais (CAMINHA e FIGUEIREDO, 2011). Uma característica chave da economia solidária é ser organizada sob a forma de auto-gestão. Logo, tal termo denota uma forma de economia, onde há atividades de produção, distribuição e consumo, bem como relações econômicas entre indivíduos e instituições (FARIA, 2010). Portanto, é algo claramente distinto do terceiro setor, onde, como já vimos, há frequentemente uma relação de cunho assistencial entre seus atores.

2.1.3 Moedas Complementares

O objetivo desta seção é chegar a um entendimento do que significam cada um dos termos frequentemente usados na literatura para se referir às moedas alternativas, enquanto moedas não oficiais, criadas por cidadãos e não pelo Estado. Como resultado desta revisão da literatura, elegeremos um termo capaz de representar todas as moedas alternativas que serão objeto de análise deste trabalho, bem como esclareceremos os critérios que motivarão a escolha de um termo abrangente e único em detrimento da diversidade de termos adotados por diferentes autores na literatura.

Diversos autores consideram que a primeira moeda dita comunitária (*community currency*, na literatura inglesa) surgiu em 1983 na Ilha de Vancouver, Colúmbia Britânica, Canadá. Essa moeda não possui um nome, sendo identificada apenas como LETS (*Local Exchange Trading System*), que pode ser traduzido como Sistema de Troca a Nível Local, ou Sistema de Troca

Local e teria sido criada por um programador desempregado chamado Michael Linton (COLLOM, 2005), (FREIRE, 2011), (BLANC, 2012), (RIGO, 2014). Esse modelo de moeda comunitária se popularizou durante toda a década de oitenta, tendo seu pico em meados dos anos noventa. A partir do LETS, outras tentativas de se criar moedas comunitárias surgiram em diversos países. Em geral, as moedas comunitárias (também chamadas sociais ou locais em diferentes trabalhos) que se seguiram ao LETS guardam diversas semelhanças entre si e com suas precursoras. A seguir, veremos brevemente como diferentes autores percebem e classificam essas experiências, bem como quais termos esses autores adotam para se referir a tais experiências.

De acordo com Collom (2005), oitenta e dois sistemas de moedas comunitárias foram criados nos Estado Unidos entre os anos de 1991 e 2005, embora pouco mais de 20% ainda estivessem em atividade à época de publicação do artigo. Collom (2005), então, investiga quais são os ambientes em que as moedas comunitárias florescem e prosperam. O autor conclui que as moedas comunitárias prosperam de forma mais longeva, ou seja, se mantém ativas e relevantes por mais tempo, em comunidades onde há baixa renda familiar, alto índice de pobreza, alto índice de desemprego e um extenso número de pessoas que trabalham por conta própria. Collom (2005) aponta para a existência de três modelos notáveis de moedas comunitárias, existentes em diversos países, não só nos Estados Unidos. O primeiro deles é o próprio LETS, os demais são os *time banks* (bancos de horas) e os sistemas *Hours*, os quais seriam moedas comunitárias semelhantes à moeda chamada Ithaca HOURS, surgida em Nova Iorque no ano de 1991, sendo esta a primeira iniciativa comunitária a adotar a impressão de papel-moeda.

Dittmer (2013), em um trabalho mais recente, ratifica as três categorias de moedas apontadas por Collom (2005) e aponta para uma quarta categoria não considerada por aquele autor, as "convertible local currencies (CLCs)", ou moedas locais conversíveis. O autor cita como exemplos de CLC a moeda *Regiogelder*, da Alemanha, e o *BerkShare*, dos Estados Unidos. De acordo com Dittmer (2013), essas moedas se assemelham ao HOURS, tendo como principal diferença a existência de lastro em moeda de cunho forçado, pela qual as CLCs podem ser trocadas.

Portanto, na literatura inglesa, o termo mais empregado para se referir às moedas alternativas surgidas nas economias locais é "community currency" (moeda comunitária). Para Collom (2005) este termo surgiu como uma forma de se referir aos sistemas locais autônomos, ou às

iniciativas que visam ao aumento da autonomia (*empowerment*) de comunidades economicamente marginalizadas. Freire (2011), em sua análise das moedas sociais em prol de um marco legal no Brasil, considera que esse termo reflete o caráter fechado de tais iniciativas, as quais seriam de tamanho reduzido e de adesão formal, embora na literatura de língua inglesa, o termo também seja empregado para designar iniciativas de adesão não formal. Consideramos, portanto, que o conceito de economia voltada à autonomia de comunidades marginalizadas é em tudo semelhante à ideia de economia solidária, frequentemente presente nos trabalhos em língua portuguesa, visto se tratar de uma forma autogestionária de economia local. A autogestão é um dos princípios mais importantes das economias ditas solidárias, senão o mais importante. Outros princípios frequentemente associados à economia solidária são: "participação, cooperação, preservação do meio ambiente, solidariedade, consumo ético e solidário" (FREIRE, 2011). Portanto, este seria um primeiro indício de que o que Collom (2005) e Dittmer (2013) chamam de "community currency" na literatura em língua inglesa designa experiências semelhantes, senão perfeitamente equivalentes, às analisadas por Freire (2011) no âmbito das economias solidárias no Brasil.

Freire (2011), entretanto, adota uma classificação diferente para as "moedas comunitárias" de Collom (2005), chamadas "moedas sociais" pela autora, dado o diferente foco, mais social, das análises conduzidas em seu trabalho. Além disso, a autora classifica aquilo que seriam os CLCs para Dittmer (2013) como "moeda social lastreada em moeda estatal". Para fins deste trabalho, contudo, decidimos adotar o termo "moeda comunitária" em detrimento do termo "moeda social", bem como adotar o termo "moedas conversíveis" (do inglês *convertible local currencies*, ou CLC) em detrimento do termo "moeda social lastreada em moeda estatal", pelos seguintes motivos: o trabalho de Freire (2011) procura enfatizar o aspecto social das moedas, enquanto o presente trabalho procura enfatizar os aspectos técnicos e procedimentais das moedas. A linha de classificação seguida por Freire (2011), embora excelente, vai na contramão do foco principal deste trabalho. Tal linha de classificação permitiria, por exemplo, agrupar *LETS* e *Hours* em uma mesma categoria, embora ambas possuam diferenças técnicas significativas para o escopo de análise deste trabalho. Acreditamos, igualmente, que a linha de classificação seguida por Collom (2005) e por Dittmer (2013) facilitaria o agrupamento das experiências em função de seus aspectos mais técnicos. Tal classificação vem ao encontro dos objetivos deste trabalho, em que se buscará identificar os aspectos técnicos inerentes às formas de organizações comunitárias, locais ou solidárias. Ou seja, buscamos neste trabalho identificar como as comunidades se constituem internamente, quais aspectos organizacionais, quais

processos internos desta organização social seriam afetados pela adoção de uma tecnologia estranha a tais comunidades, como é o Bitcoin. Logo, consideramos que o termo "moeda social", frequentemente empregado na literatura brasileira é, para fins das análises a serem conduzidas neste trabalho, equivalente ao termo "moeda comunitária" da literatura inglesa. Dado que uma análise histórica apontará para a precedência das iniciativas econômico-solidárias surgidas nos países de língua inglesa sobre as experiências surgidas nos demais países, decidimos adotar "moeda comunitária" como a terminologia preferida entre as duas opções.

Entretanto, o termo "moeda comunitária" não figura exclusivamente nem mesmo na literatura inglesa, onde os termos "moeda local" e "moeda complementar" também aparecem com frequência. O termo "moeda complementar" será analisado em breve. Cabe observar, de imediato, que o termo "moeda local", foi evitado neste trabalho por enfatizar excessivamente o aspecto de abrangência territorial de uma moeda. A análise exclusivamente em termos de extensão, ou alcance territorial de uma moeda não é objeto de estudo deste trabalho, e tal termo poderia ressaltar tal aspecto em demasia (BLANC, 2011). Cabe também frisar que o termo "moeda alternativa" também foi evitado, sendo usado propositalmente em momentos específicos como um termo totalmente genérico. Essa escolha se deu em benefício de uma maior clareza, já que este termo frequentemente se confunde com o termo "moeda paralela", que é excessivamente amplo, sendo frequentemente usado para se referir, inclusive, às moedas virtuais criptográficas, as quais também são objeto de estudo deste trabalho, sem contudo em momento algum figurarem no mesmo grupo das moedas comunitárias ou sociais para fins de análise. Portanto, foi necessário encontrar na literatura um termo que fosse capaz de agrupar todas as experiências locais, comunitárias ou sociais analisadas sem que se assumisse um escopo excessivamente extenso.

Rigo (2014) aponta o termo "moeda cidadã" como sendo uma tendência na literatura francesa. A intenção deste termo seria explicitar a autonomia do cidadão na criação e execução das políticas de tal moeda, que podem ser políticas com fins sociais, ecológicos, culturais ou mesmo comerciais. Embora este termo nos pareça bastante apropriado, ele não é atualmente adotado pelo *International Journal of Community Currency Research* (IJCCR), que foi uma das fontes primárias de pesquisa neste trabalho. Portanto, decidimos nos restringir aos termos de maior uso corrente. Em nossa visão, portanto, o termo "moeda cidadã" teria um escopo amplo e genérico o suficiente, porém, a adoção de tal termo dificultaria o estabelecimento de um vínculo com trabalhos importantes citados no corpo deste trabalho. Blanc (2012) em sua compilação de

artigos publicados nos últimos trinta anos no IJCCR utiliza os termos “moedas comunitárias” e “moedas complementares” para se referir ao conjunto de todas as experiências relatas na publicações compiladas.

Entretanto, Blanc (2011) torna explícita a existência de certa discordância na comunidade acadêmica a respeito dos termos “moedas comunitárias” e “moedas complementares”. O autor, então, propõe uma classificação metódica e abrangente e define o que é CC (*Community Currency* / *Complementary Currency*) e o que não é, ou seja, o que deve ser considerado como parte do conjunto de experiências de moedas criadas por cidadãos e o que é externo a tais sistemas. Cabe notar que a ambiguidade da sigla CC, a qual ao mesmo tempo pode se referir a *community currency* ou a *complementary currency* é vista por Blanc (2011) como uma forma de evitar o conflito de interpretações entre autores com visões diferentes, pois a sigla não deixa explícita qual a visão específica de Blanc. Entretanto, como reconhece o autor, tal artifício não funciona em línguas latinas ou em outros idiomas. Permanece, portanto, a necessidade de uma classificação mais assertiva, a qual é objeto do trabalho do autor. Blanc (2011) conclui, a partir de modelos ideias, que há três níveis de experiências com filosofias distintas: moedas locais, moedas comunitárias e moedas complementares. Essas três categorias de experiências seriam suficientes para definir o conjunto do que é “CC”, ou seja, daquilo que são iniciativas cidadãs que tem como filosofia o desenho ou o redesenho das relações de troca, distribuição de bens e reciprocidade entre indivíduos. Moedas estatais ou moedas com fins exclusivamente comerciais estariam fora desse conjunto. O autor considera ainda que moedas locais teriam como característica principal sua relação com espaços geopolíticos, enquanto moedas comunitárias seriam pautadas pela relação com espaços sociais, sejam eles comunidades formalmente constituídas ou comunidades *ad hoc*. Por fim, moedas complementares seriam as experiências de escopo mais amplo, que lidam com espaços econômicos, onde as relações de produção e troca são enfatizadas (BLANC, 2011).

Entretanto, Collom (2011) defende que os termos “moeda local” e “moeda comunitária” são subcategorias que se encontram aninhadas sob o termo mais amplo, “moeda complementar”. Este termo, moeda complementar, do inglês “complementary currency”, surgiu posteriormente na literatura (SCHROEDER, MIYAZAKI e FARE, 2011) e, portanto, não figurava no trabalho de Collom (2005) citado anteriormente. Rigo (2014) citando Blanc (1998) afirma que o termo “moeda complementar” designa tipicamente um conjunto mais diversificado de experiências, incluindo moedas com fins comerciais. Entretanto, à luz de Blanc (2011), como visto no parágrafo anterior, a finalidade comercial nesse caso não poderia ser maior que a finalidade

comunitária ou social, caso contrário, tal moeda seria simplesmente uma ferramenta comercial e não seria uma "moeda complementar" no conceito de Blanc (2011). Já Freire (2011) considera que o termo "moeda complementar" reflete o alcance territorial de tais moedas, as quais não estariam necessariamente circunscritas a uma pequena comunidade, mas estariam abertas à participação de grupos mais amplos, ou seja, o termo representaria experiências ao mesmo tempo comunitárias, mas com abrangência territorial ampla, sem que seja exigida uma adesão formal ao sistema. Esse escopo mais amplo do termo "moeda complementar", proposto por ambos Collom (2011) e Freire (2011), serve melhor ao propósito deste trabalho, pois não pretendemos restringir as análises a serem conduzidas em termos sociais, nem em termos geográficos, nem tampouco em termos da ausência de lucro nos sistemas analisados. Cabe frisar que a existência de lucro como uma parte do sistema não transforma a moeda necessariamente em uma moeda comercial (*for-profit currency*). Portanto, decidimos eleger o termo "moeda complementar" como sendo capaz de agrupar os conceitos de "moeda comunitária" (bem como "moeda social") e "moeda local", sendo mais específico que o termo "moeda alternativa" e possivelmente equivalente ao termo "moeda cidadã" citado por Rigo (2014). Cabe ressaltar que qualquer menção a "comunidade" neste trabalho ocorrerá em termos genéricos. Portanto, para fins das análises conduzidas neste trabalho, comunidade é qualquer grupo de indivíduos que possa ser identificado a partir das relação econômicas e sociais de que participam. A existência dessa relação entre indivíduos pode se constituir de maneira formal ou informal, tendo fins lucrativos ou exclusivamente solidários. O importante para fins das análises conduzidas neste trabalho é que existam atores responsáveis pela emissão e administração de uma moeda e que existam pessoas que aceitem e utilizem tal moeda, incluindo ou não os próprios atores que a criaram. Portanto, neste trabalho "moeda complementar" desponta como o termo mais adequado para designar o conjunto de moedas locais, sociais, comunitárias e, inclusive, complementares, aqui em sentido estrito, conforme Blanc (2011).

2.1.4 Moedas Criptográficas

Na literatura, moedas criptográficas são às vezes chamadas moedas virtuais ou moedas eletrônicas, dado que sua existência é eminentemente imaterial, ou seja, existem na forma de informação codificada em dispositivos eletrônicos, frequentemente em computadores. Entretanto, discordamos da equivalência entre os termos virtual e criptográfica, pois consideramos que moedas virtuais podem não fazer uso de criptografia, assim como moedas criptográficas podem não ser virtuais, embora geralmente o sejam. Um exemplo de moedas

virtuais não necessariamente criptográficas são as moedas utilizadas em jogos eletrônicos, como as moedas usadas em MMORPGs. Tais moedas se caracterizam por serem uma forma de se codificar dados digitalmente a fim de representar a posse da moeda e as transações entre indivíduos por meio da manipulação desses dados. (KIM, 2015). Logo, uma moeda virtual pode ser uma moeda criptográfica, e uma moeda criptográfica pode ou não ser uma moeda virtual. Há formas de se implementar uma moeda criptográfica usando o papel, isso já foi realizado com o Bitcoin, embora dados os valores da comunidade responsável pelo Bitcoin, sobretudo a valorização da privacidade e da segurança, tal prática é desencorajada. Além disso, no caso do Bitcoin, o uso da moeda em papel não dispensa o uso posterior do computador, pois todas as transações devem ser validadas de forma eletrônica, como veremos em mais detalhes a seguir (Paper Wallet, 2016).

A moeda criptográfica mais notável, tanto em termos de estudos existentes, nos campos técnico, teórico e jurídico, quanto em termos de valor de mercado é o Bitcoin. O Bitcoin, além de ser a primeira moeda virtual criptográfica criada e que, portanto, inspirou tanto a nível técnico como teórico as diversas outras moedas criptográficas existentes, é também aquela que apresentou maior desenvolvimento, como a introdução de inovações conceituais em cima da infraestrutura existente. Um exemplo de inovação neste sentido, é a possibilidade de se colorir as moedas virtuais, conceito que será aprofundado a seguir. Neste trabalho priorizaremos a análise do papel do Bitcoin na criação de moedas comunitárias, favorecendo essa moeda sobre as demais moedas criptográficas existentes. Essa escolha se deu principalmente em razão do fato de que a capacidade de se "colorir" moedas é, atualmente, exclusiva do Bitcoin, e a ausência de tal possibilidade tornaria impossível as considerações e análises realizadas neste trabalho.

Entretanto, cabe aqui um questionamento: O Bitcoin e as moedas criptográficas exercem realmente todas as funções de uma moeda e, de fato, podem ser consideradas moedas? Lee *et al.* (2015) consideram que o maior obstáculo para que as moedas criptográficas possam ser, de fato, consideradas moedas é a alta volatilidade de seu valor e a dualidade de tratamento que elas tem recebido até o momento, ora como meio de investimento especulativo, ora como meio de se realizar transações entre indivíduos. No Brasil, tanto o Bitcoin quanto o Litecoin, ou qualquer outra moeda criptográfica, são considerados "bens" ou "direitos", assim como o ouro ou outros ativos financeiros, não moedas (ONGARATTO, 2016). Entendimento semelhante é adotado nos Estados Unidos, onde as moedas criptográficas são consideradas um meio de troca que opera como moeda em alguns contextos, mas que carece de todas as características de uma moeda real. Notavelmente, tais moedas não possuem curso legal em nenhum país e, portanto,

podem ser livremente rejeitadas como meio de pagamento. Portanto, para fins de tributação, tais moedas são tratadas como propriedade, como bens, nos Estados Unidos (LEE, LONG, *et al.*, 2015). Levando-se em consideração que as moedas criptográficas não possuem curso legal em nenhum país, é de se esperar que elas sejam tratadas oficialmente como bens em todos os países que tenham definido o caráter dessas moedas para fins de tributação. Entretanto, o fato de tais moedas serem tratados como bens não é um impeditivo para que sejam usadas para outros fins, como será discutido na seção seguinte. Antes disso, porém, devemos ainda no aprofundar um pouco mais no que é o Bitcoin com base na literatura existente.

Satoshi Nakamoto lançou o Bitcoin em Fevereiro de 2009 no fórum P2P Foundation, sob a alcunha de "uma implementação de código aberto de uma moeda P2P" (NAKAMOTO, 2009). Pela postagem original de Nakamoto, é possível perceber que havia duas preocupações essenciais, dois problemas a serem resolvidos pelo Bitcoin. O primeiro problema é a confiança nas instituições bancárias. Em nome da segurança, a moeda de cunho forçado, de aceitação obrigatória, precisa ser garantida por uma instituição terceira, os bancos. Portanto, para que se tenha um sistema seguro, abre-se mão da privacidade, deixando dados bancários, nome, número de identificação, valores de depósito, número de cartões de crédito sob a tutela de uma instituição que garantirá a segurança das transações entre dois particulares. O Bitcoin procura resolver este problema por meio da descentralização, já que o protocolo é implementado sob uma rede P2P. O segundo problema é o problema dos custos. Todo esse arcabouço das instituições bancárias possui um custo alto de manutenção, isso quase sempre impossibilita a realização de micro pagamentos, pois estes se tornam inviáveis economicamente. Serve como evidência anedótica, a prática comum, realizada por vários estabelecimentos comerciais, de se recusar o pagamento via cartão de crédito caso o valor da compra seja muito baixo, por exemplo, abaixo de 10 reais. Abaixo, segue-se uma citação que evidencia de forma perfeitamente sucinta a motivação principal do Bitcoin:

> The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve. We have to trust them with our privacy, trust them not to let identity thieves drain our accounts. Their massive overhead costs make micropayments impossible. (NAKAMOTO, 2009)

> A raiz do problema com as moedas convencionais é toda a confiança que é necessária para fazer isso funcionar. É necessário ter confiança de que o banco central não degradará a moeda, mas a história da moeda fiável é cheia de quebras nessa confiança. É necessário confiar no bancos para que guardem nosso dinheiro e os transfiram eletronicamente, mas eles emprestam esse dinheiro em ondas de bolhas de crédito ficando com mal uma fração de reserva. Nós somos obrigados a confiar a eles nossa privacidade, acreditar que eles não deixarão ladrões de identidade drenarem nossas contas. A sobrecarga maciça dos custos deles tornam micro pagamentos impossível. (NAKAMOTO, 2009) - em tradução nossa

Para concluir esta seção, explicaremos brevemente a mecânica interna de funcionamento do Bitcoin, apenas para que se torne mais fácil entender a discussão que vem imediatamente a seguir, já que este assunto será melhor explorado futuramente no corpo deste trabalho. Para fins desta breve explicação, usaremos o *paper* de Nakamoto como base, pois este é o trabalho original, o qual dá base teórica para qualquer implementação do Bitcoin e para qualquer análise aprofundada do funcionamento deste protocolo. Na prática, caso um cliente Bitcoin (um software usado para se conectar à rede P2P do Bitcoin) não siga o projeto de Nakamoto, ele não funcionará, pois todas as transações originadas neste dado cliente serão recusadas pelos demais membros da rede. Portanto, não há implementações alternativas, concorrentes, dentro do que é aceito pela rede Bitcoin. Até mesmo as demais moedas criptográficas existentes, tendo sido inspiradas no Bitcoin, compartilham muitas características de projeto (*design*) com o Bitcoin.

Em seu cerne, o Bitcoin substitui a autoridade bancária por uma rede peer-to-peer (P2P). Isso significa que não há autoridade responsável por validar as transações realizadas em bitcoins, tal validação é feita por um nó qualquer da rede, o qual comunica todos os demais nós via *broadcast*. Cabe ressaltar aqui que Bitcoin com b maiúsculo se refere ao protocolo, enquanto bitcoin com b minúsculo se refere à moeda. Portanto, ao invés de confiar em uma autoridade central, o Bitcoin confia na rede de usuários, ou rede P2P. Cada nó da rede, ou cada usuário pode validar transações, para isso basta agrupá-las em um bloco e executar os algoritmos de validação padrão do protocolo. Como recompensa por esse trabalho de validação, o nó receberá um pagamento em *bitcoins*. Nakamoto assume que o protocolo será confiável enquanto houver mais nós na rede tentando validar transações que fraudá-las. O autor assume ainda que caso um nó específico detenha poder computacional maior que o de todos os demais nós somados, esse nó obteria maior vantagem ao se juntar à rede como um nó legítimo e receber pagamentos em bitcoins, do que ao sabotar a rede e destruir para sempre a confiança que se tem no protocolo.

O parágrafo anterior explorou a premissa básica de funcionamento do Bitcoin. Entretanto, tal premissa não é suficiente para que o Bitcoin funcione, pois ela por si só cria algumas

vulnerabilidades, às quais eram conhecidas pelo criador do Bitcoin, e levaram o projeto ou *design* do Bitcoin a ser da forma que é. No protocolo Bitcoin a moeda nada mais é que informação, dados escritos em um arquivo eletrônico, facilmente manipuláveis. Portanto, como evitar a falsificação de moeda? Uma parte da solução proposta por Nakamoto foi o uso de assinaturas digitais. As assinaturas digitais são utilizadas em todas as transações realizadas, de modo a formar uma cadeia de validação. Ou seja, a transação atual se torna dependente da transação anterior. Essas transações devem ser agrupadas em blocos para que sejam validadas, como já explicamos no parágrafo anterior. Todos os blocos de transações carregam um *hash* (uma cadeia de caracteres única) gerado a partir do bloco anterior. E todos os blocos se conectam um aos outros por meio desse *hash*, formando uma cadeia única, a *block chain*. Portanto, caso alguém queira falsificar bitcoins, seria necessário alterar todo esse legado, alterar o bloco anterior, onde as bitcoins falsificadas não existiam e torna-las existentes naquele bloco. Entretanto, como a rede P2P funciona de forma independente, outras pessoas estariam a validar operações e estariam usando aquele bloco anterior, já validado, como base para o hash. Portanto, o falsificador teria que, ao mesmo tempo em que altera o bloco anterior, validar o bloco atual, para que este se torne o próximo bloco "oficial" a ser integrado à cadeia de blocos (*block chain*), a qual é única, compartilhada por todos os nós da rede. Logo, percebe-se que a *block chain* é o principal componente técnico do Bitcoin, sendo o coração do funcionamento seguro do Bitcoin. É este componente que permite que outros autores especulem a respeito ou proponham diferentes usos para o Bitcoin, que é o que veremos a seguir.

2.2 Moedas Criptográficas como Moedas Complementares

Um dos trabalhos pioneiros, senão o primeiro autor, a propor o uso de uma moeda criptográfica virtual como moeda local é o *paper* auto publicado do matemático israelense Meni Rosenfeld. A importância deste trabalho reside em ser, o trabalho original em que foi definido o arcabouço teórico para o uso de *colored bitcoins*, também chamadas colored coins, podendo ser traduzido como bitcoins coloridas ou moedas coloridas (BUTERIN, 2013). Essa técnica proposta por Rosenfeld (2012) se trata de uma forma simples de adicionar metadados às bitcoins comuns. Assim, seria possível se beneficiar da infraestrutura do Bitcoin, notavelmente, se beneficiar da irreversibilidade das transações realizadas, a fim de guardar de forma cronológica e permamente outras informações importantes. Deste modo, seria possível, na visão do autor, criar moedas comunitárias em cima da infraestrutura do Bitcoin. Essas moedas seriam nada mais que *bitcoins* com uma "marca" especial, com uma "cor", com uma informação extra

atrelada a ela. Entretanto, o foco do trabalho de Rosenfeld é definir o arcabouço teórico e propor, ao mesmo tempo, diversos usos possíveis, sem dar muitos detalhes sobre cada um. Cabe frisar que será discutido posteriormente no corpo deste trabalho o mérido dos termos "moeda local" e "moeda comunitária" empregados por Rosenfeld em seu trabalho. O autor cita como outros usos possíveis dessa inovação a emissão de certificados de propriedade, empréstimos, ou até mesmo emitir ações de uma companhia (ROSENFELD, 2012). Entretanto, embora tal proposta seja tentadora *a priori*, e aparentemente já tenha sido adotada por um banco finlandês chamado LHV, o qual de acordo com a *bitcoinwiki* teria emitido um valor superior a 100.000 euros em empréstimos bancários por meio de *colored* bitcoins, há ainda pouquíssimos estudos que tenham analisado o uso de tal inovação, e nem mesmo dentro da comunidade Bitcoin o tópico é incontroverso, havendo dissidências em torno de sua adoção permanente devido à sobrecarga que a introdução de informação extra implica no funcionamento do protocolo. O maior problema é que os nós da rede Bitcoin realizam o trabalho de validar blocos de transações a fim de serem recompensados com pagamentos em bitcoins. Entretanto, não faz parte do "contrato" original aceitar e validar tacitamente outras informações, metadados, os quais adicionam uma sobrecarga de dados sem prover qualquer benefício para os nós que os validam. Inicialmente, nos primeiros anos de adoção das *colored* bitcoins, 80 bytes de metadados podiam ser adicionados a cada "bitcoin" (o uso de aspas aqui se deve ao fato de que a forma de se adicionar metadados pode variar, sendo usualmente adicionados à transação, ou seja, são adicionados a uma bitcoin de forma indireta), valor que foi cortado pela metade pela comunidade Bitcoin a fim de reduzir a sobrecarda de informação não pertinente (ou extra) sendo adicionada à cadeia de transações (*block chain*) original do Bitcoin (ANDERSEN, 2014).

O trabalho de Garay, Kiayias & Leonardos (2015) analisa o núcleo do protocolo Bitcoin e investiga as possíveis aplicações para o que eles definem como a espinha-dorsal do Bitcoin. Pode-se considerar que esses autores buscaram aplicar o rigor científico em sua análise, algo que falta no trabalho de Rosenfeld, o qual parte de uma visão muito mais pragmática de alguém que possui fortes ligações com a comunidade Bitcoin, já que o próprio Rosenfeld é um dos organizadores da comunidade Bitcoin em Israel (BUTERIN, 2013). O protocolo Bitcoin se caracteriza por construir, à medida que transações são realizadas, uma cadeia de blocos de transações, a chamada *block chain*. Essa cadeia de blocos de transações é compartilhada por todos os nós da rede, ou seja, cada pessoa utilizando o Bitcoin terá uma cópia dessa cadeia contendo todas as transações já realizadas em bitcoins, as quais estão agrupadas em blocos. De forma bastante resumida, a espinha-dorsal do Bitcoin, coforme definida por Garay, Kiayias e

Leonardos, seria o conjunto de algoritmos executados por um dado nó a fim de: 1. validar a cópia da cadeia de transações que este nó possui como sendo a mais recente aceita pela rede P2P; 2. comparar duas possíveis cadeias a fim de definir qual é "a melhor", quando houver mais de uma cadeia sendo temporariamente adotadas pela rede P2P; 3. resolver um problema matemático complexo como condição para que se possa estender a cadeia oficial do Bitcoin, ou seja, adicionar um bloco validado à *block chain*. Todos esses conceitos serão melhor explicados posteriormente no corpo deste trabalho.

Garay, Kiayias & Leonardos (2015) apresentam duas conclusões principais. A primeira é que o Bitcoin pode ser usado para se implementar acordos Bizantinos. O termo "acordo Bizantino" é a definição formal usada em computação distribuída para um dos problemas discutidos por Nakamoto de forma menos formal em seu *paper*. O problema diz respeito à obtenção de consenso quanto ao que é correto em uma rede onde há nós honestos e nós maliciosos. Nakamoto (2009) defende que a probabilidade de que um atacante (um nó malicioso) consiga tomar a liderança na cadeia de blocos "oficiais" do Bitcoin, ou seja, de blocos válidos adotados por todos os demais nós da rede, cai exponencialmente. Garay, Kiayias e Leonardos (2015) fazem uma análise mais formal e concluem que uma maioria de nós honestos com igual poder computacional é suficiente para que se mantenha a rede livre de ataques, desde que a rede tenha capacidade de se mater sincrozinada em um tempo rápido o suficiente quando comparado à capacidade de os nós atacantes validarem blocos e enviá-los para toda a rede. A segunda conclusão dos autores, afirma que o Bitcoin pode ser um robusto "livro razão público" (*transaction public ledger*). Esta conclusão é importante, pois é justamente essa a premissa adotada por Rosenfeld (2012) ao propor suas *colored coins*. Em resumo, o Bitcoin funciona como um livro razão público, um livro de acesso aberto a todos onde se registram todas as transações realizadas de forma sequencial e irreversível. Esse aspecto de irreversibilidade depende do número de transações realizadas após uma determinada transação ser registrada no "livro". Tipicamente, na comuniade Bitcoin, se considera que uma sequência de seis blocos de transações validadas é suficiente para que se considere uma operação como "irreversível".

Entretanto, a publicação que apresenta maior proximidade com o tema deste trabalho, qual seja o uso de moedas criptográficas no contexto de uma moeda comunitária, é o artigo de Vandervort, Gaucas & Jacques (2015). Nesse trabalho os autores propõem uma adaptação do protocolo Bitcoin, a fim de se atender a necessidades específicas de moedas comunitárias, com foco em comunidades onde é necessário realizar votações. Os autores propõem um sistema de votação

que seria implementado nos moldes do Bitcoin, fazendo uso de uma cadeia de validação (*block chain*) e de uma rede P2P (VANDERVORT, GAUCAS e JACQUES, 2015). Portanto, pode-se considerar que o trabalho de Vandevort, Gaucas e Jacques (2015) vai ao encontro da análise feita por Garay, Kiayias e Leonardos (2015), porém ignora a proposta de Rosenfeld (2012), pois decide utilizar o Bitcoin como modelo de solução, mas não como infraestrutura, como base direta, para uma solução. Tal escolha pode ter se dado apenas em função de os autores terem eleito a realização de votações comunitárias como foco de sua análise, mas não fica claro se os autores tinham ou não conhecimento das colored bitcoins propostas por Rosenfeld, às quais, de uma forma ou de outra, não seriam adequadas para a realização de votações comunitárias, como desejavam os autores.

3 MOEDAS COMPLEMENTARES COMPARADAS

3.1 Definição das Classes de Moedas Complementares

Dentre os autores consultados durante a escrita deste trabalho, apenas Blanc (2011) realiza uma classificação metódica dos "projetos" com finalidades econômico-sociais, neste trabalho chamados de "moedas complementares". Entretanto, a classificação proposta por Blanc (2011) é meramente tipológica e, portanto, foi de grande importância como referencial teórico durante a revisão da literatura, bem como na escolha do termo "moeda complementar" como termo de referência neste trabalho. Contudo, o objetivo desta seção é classificar as moedas complementares em função de seus aspectos técnicos, a fim de que possamos na seção seguinte analisar a compatibilidade de cada classe de moeda complementar a ser aqui definida com as *colored bitcoins* de Rosenfeld (2012). É interessante apresentar, aqui, a justificativa de tal análise. Vejamos, nas palavras do próprio Rosenfeld (2012): "*a community may want to use a local currency which is similar technically to Bitcoin but detached from it monetarily*". Em tradução livre, isso significa que, na proposta original de Rosenfeld (2012) fica aberta a possibilidade de se usar as "bitcoins coloridas" para criar uma "moeda local" desde que haja similaridade técnica desta com aquela. Ora, o que seria, então, esta similaridade técnica? Como isso pode ser avaliado? O trabalho de Rosenfeld é extremamente omisso a este respeito, fato que será discutido em maior profundidade posteriormente, mas já fica clara a necessidade se ter uma forma, um arcabouço para que se possa avaliar, ainda que somente de forma qualitativa, se há realmente uma viabilidade técnica e, porque não, uma compatibilidade de filosofias, de princípios e valores entre moedas complementares e *bitcoins*. Tais questões, portanto, serão norteadoras das análises conduzidas a partir deste capítulo.

Varrer a literatura em busca de aspectos técnicos das moedas complementares não é uma tarefa trivial. A esmagadora maioria, senão todos os autores pesquisados, tendem a se focar em aspectos comunitários e sociais de tais experiências, visto que os aspectos técnicos, os processos e procedimentos administrativos internos de uma moeda complementar, não são o tema central de seus trabalhos. Entretanto, é possível colher informações técnicas sobre as moedas complementares, ainda que de forma dispersa, a partir do trabalho de diversos autores, de forma complementar. Alguns autores classificam as moedas em função de algum aspecto interno de seu funcionamento, e tal classificação facilita sobremaneira a categorização proposta por este trabalho. Por exemplo, Freire (2011) divide as moedas comunitárias primeiramente em duas grandes categorias, "moedas sem lastro em moeda oficial" e "moedas com lastro em moeda oficial". De acordo com a autora, os sistemas *LETS* são uma forma evoluída de escambo, a qual se beneficia do uso de computadores para eliminar a obrigatoriedade de se encontrar uma correspondência direta e imediata de um item por outro para fins de troca. Em tais sistemas há um profissional da contabilidade que atua como intermediário nas trocas entre dois membros, realizando o débito na conta do comprador e o crédito na conta do vendedor em unidade monetária comum, ou seja, aquela adotada pela comunidade. A autora defende ainda que o sistema Hours, assim como o *LETS*, funciona de forma semelhante ao escambo. Portanto, ambos se caracterizam por não possuírem lastro em moeda oficial. Entretanto, cabe frisar que o sistema Hours possui uma diferença significativa, a impressão de papel moeda, o que altera completamente a organização interna deste sistema, como veremos em breve. Portanto, não seria útil conduzir esta classificação a partir da visão de cada autor, mas sim a partir daquilo que frequentemente é identificado como moeda complementar por diferentes autores e como eles as definem.

Os dois sistemas de moedas complementares mencionados no parágrafo anterior, o *LETS* e o Hours, são citados por todos os autores estudados, portanto são um bom ponto e partida. Freire (2011) apresenta, citando diversos autores, uma descrição detalhada do funcionamento do sistema Hours. A autora introduz esse sistema como sendo uma forma evoluída do *LETS*, em que os dois gargalos principais do sistema anterior foram resolvidos por meio da emissão de papel-moeda. Ao se adotar a emissão de papel moeda, eliminou-se a necessidade de se ter uma central contábil responsável por registrar todas as transações, bem como eliminou-se a necessidade de que todas as ofertas e procuras dos membros da comunidade fossem cadastradas e divulgadas periodicamente em uma lista, já que com a introdução do papel-moeda cada

membro da comunidade se tornou livre para negociar com seus pares e efetuar pagamentos. Entretanto, a emissão de papel-moeda, consequentemente, eliminou o equilíbrio entre débitos e créditos existente no sistema *LETS*, já que a comunidade decide a quantidade de papel-moeda a ser impressa, bem como pode aprovar concessões de empréstimos. Tais características tornam a dinâmica interna do sistema Hours bastante diferente daquela do sistema *LETS*, onde uma moeda (virtual) é criada somente a partir de uma transação realizada como mero meio de registro contábil. Logo, o sistema *LETS* funciona com base em um constante equilíbrio de débitos e créditos, onde não há empréstimos, embora um participante possa "gastar" créditos e ficar com saldo devedor indefinidamente. Veremos a seguir, então, de forma sintética o que são esses dois sistemas.

Definições bastante completas e sumárias do que são os sistemas *LETS* e Hours podem ser encontradas em Dittmer (2013), o qual resume de forma perfeitamente concisa boa parte das informações presentes em trabalhos de outros autores. *LETS* significa Sistema de Troca Local, ou Sistema de Troca a Nível Local (do inglês Local Exchange Trading Systems). O primeiro *LETS* surgiu em *Vancouver Island* em 1983 como reação a uma recessão econômica. Tratam-se de sistemas de trocas, ou clubes, nos quais seus membros podem trocar bens ou serviços com base em uma moeda virtual, a qual pode usar a moeda oficial como referencial contábil para fins de registro. Há uma central contábil, geralmente composta por voluntários, responsável por cadastrar os participantes e registrar as transações realizadas. Todos os participantes começam com saldo zerado e a cada transação, a cada "troca", credita-se o fornecedor e debita-se o tomador do bem ou serviço. Os balanços individuais das contas podem ser publicados, bem como pode-se estabelecer limites de débito a fim de evitar abusos e exploração maliciosa do sistema. Nesses sistemas é necessário divulgar periodicamente as ofertas e demandas de bens e serviços para que os participantes possam ter conhecimento da existência um dos outros enquanto membros do sistema. Notavelmente, esses sistemas se espalharam durante a década de 1980 pelo Reino Unido, Austrália, Nova Zelândia e Alemanha.

Já o sistema Hours, embora inspirado no *LETS*, caracteriza-se pela impressão de papel-moeda sem lastro em moeda oficial. A experiência mais conhecida, a qual dá nome a esse sistema, é a moeda *Ithaca* HOURS, surgida na cidade de *Ithaca, New York*, nos Estados Unidos em 1991. Assim como o *LETS*, esse sistema foi criado como resposta a uma recessão econômica. A ideia era criar um meio de troca mais fluido que o *LETS*, que prescindisse da necessidade de uma central contábil, embora o Hours também requeira administração ativa. O fato de o sistema ser bem administrado, com um controle central da emissão de moeda, foi justamente o que atraiu

a confiança de negócios locais, os quais começaram a aceitar a moeda, algo que não existe nos sistemas *LETS*. Por fim, cabe notar que o nome da moeda HOURS (que poderia ser traduzido do inglês como HORAS) pode conduzir a um entendimento equivocado do valor da moeda. O valor de referência do Ithaca HOURS era o valor médio da hora de trabalho na cidade de *Ithaca*, 10 dólares americanos. O nome HOURS foi escolhido tendo como filosofia o princípio do valor igualitário da mão-de-obra, mas a escolha desse nome nunca teve a intenção de estabelecer um referencial absoluto de preço, isto é, uma hora de trabalho poderia, a critério das partes de uma transação, ser paga com mais do que uma cédula com valor de 1 Ithaca HOUR (DITTMER, 2013). Ainda a respeito do valor da mão-de-obra, há uma outra diferença significativa entre o *LETS* e o Hours é que no sistema *LETS* é comum haver discordâncias quanto ao preço, ou quanto à equivalência de valor da mão-de-obra, pois o sistema *LETS* tipicamente assume um valor equivalente de trabalho/hora para todos os participantes, sem considerar as diferenças na qualidade ou no nível de habilidade de cada prestador de serviço (DITTMER, 2013). No sistema Hours, como vimos, isto não ocorre, pois as partes de uma transação ficam livres para discutir de forma totalmente independente o valor a ser pago por um serviço. Caso se decida pagar um valor maior (ou um valor menor) que o valor de referência pela hora de trabalho (USD 10,00/hora), basta ajustar a diferença usando o papel-moeda. Inclusive, a forma como o papel-moeda do *Ithaca* HOURS foi projetado torna explícito o quanto se está desviando do valor de referência, pois as notas emitidas possuem valores equivalentes a frações de hora, desde um décimo de hora (equivalente a 1 dólar) a duas horas (equivalente a 20 dólares) (COLLOM, 2005).

Entretanto, entre a criação do *LETS* e o surgimento do Hours, um outro sistema de troca notável foi criado. Esse sistema é conhecido na literatura como *time banks*, ou bancos de horas. De acordo com Collom (2005) os t*ime banks* e os *LETS* guardam maiores semelhanças entre si do que com o sistema Hours, pois nos dois primeiros não há impressão de papel moeda e o sistema exige um cadastro prévio dos participantes, algo que não ocorre no sistema Hours. Nesses dois sistemas geralmente há a necessidade de se ter uma coordenação ativa, realizando o registro de todas as transações, embora isso nem sempre ocorra nos *time banks* (FRAňKOVÁ, FOUSEK, *et al.*, 2014). Segundo Collom (2005), a diferença principal entre esses dois sistemas seria que os t*ime banks* possuem forte vínculo com o trabalho voluntário, visando ao aumento do protagonismo dos indivíduos na transformação de sua realidade, sendo um meio de se opor assistencialismo por meio do incentivo ao protagonismo dos indivíduos assistidos. Logo, os

time banks assumem frequentemente um vínculo com instituições públicas ou privadas, como escolas e hospitais. Dittmer (2013) define os *time banks* como sistemas surgidos nos Estados Unidos em meados dos anos 1980 como uma forma de tornar os serviços de promoção do bem estar social mais efetivos. Assim como os *LETS*, esses sistemas se caracterizam pela prevalência das relações pessoa-a-pessoa. A missão dos organizadores do sistema é simplesmente facilitar esse contato entre os participantes e manter registro das relações de débito e crédito. Entretanto, nos time banks a evolução da relação solidária entre seus participantes muitas vezes resulta no não registro das transações, que passam a ser vistas por seus participantes mais como relação de amizade e solidariedade que como uma troca comercial propriamente dita (FRAňKOVÁ, FOUSEK, *et al.*, 2014). Os time banks, por sua origem, se caracterizam fortemente pelo envolvimento de instituições *mainstream*, como instituições dos setores educacional, hospitalar e serviços civis ou judiciais/carcerários. Segundo Dittmer (2013), além dos *time banks* pessoa-a-pessoa existem os *time banks* pessoa-a-instituição e, com bem menos frequência, instituição-a-instituição. Tipicamente, em um *time bank* pessoa-a-institução, uma instituição daria créditos aos participantes como recompensa pelo seu engajamento em comportamentos desejados (como a participação em algum evento ou a administração de algum grupo comunitário). A premissa é a mesma nos time-banks do tipo instituição-a-instituição, créditos serão concedidos pela prestação de serviços considerados importantes por uma das partes, os quais podem ser realizados sem grandes custos, sem a necessidade de uma recompensa imediata, pela outra parte. Os créditos tipicamente poderão ser trocados posteriormente por bens ou serviços. A maior crítica aos *time banks*, a qual pode explicar o reduzido volume de trabalhos publicados em comparação com os *LETS*, é o seu suporte direto a instituições já estabelecidas, e a relações sociais já existentes, enquanto os *LETS* representariam iniciativas mais radicais e, teoricamente, seriam formas mais efetivas de construção das relações sociais onde elas se fazem necessárias (DITTMER, 2013).

Rigo (2014) faz uma análise bastante completa das moedas comunitárias existentes no Brasil e faz um contraponto com as experiências relatadas em outros países. Para fins de da classificação proposta por este trabalho, procuramos identificar as semelhanças das experiências brasileiras com as experiências estrangeiras, sobretudo com os tipos de moedas identificados previamente, quais sejam, os *LETS*, *time banks*, Hours e *CLCs*. Sem dúvida a experiência mais notável no Brasil é a do Banco Palmas, surgido no conjunto Palmeiras, em Fortaleza, Ceará, em 1998. O "banco" surgiu e se solidificou como um modo de fazer frente aos problemas de baixa renda e de desemprego dos moradores do conjunto Palmeiras, fazendo uso do Crédito Produtivo e do

Crédito para Consumo como formas de movimentar a economia local, criar e manter relações de consumo dentro das fronteiras daquela comunidade. A iniciativa se multiplicou e, em 2012, tinha se transformado em uma rede de 78 Bancos Comunitários de Desenvolvimento (BCDs) espalhados por todo o país, os quais utilizam suas respectivas "moedas sociais circulantes locais" como instrumento de promoção social, por meio do acesso a crédito para o consumo e para a produção local. A respeito do termo "moeda social", o qual já discutimos anteriormente, Rigo (2014) citando Lietaer e Kennedy (2010) dá a entender que essas moedas sociais podem ser vistas como uma subclasse específica de moeda complementar, com características particulares, ao lado de outras formas semelhantes como as moedas locais, regionais, solidárias ou comunitárias, o que vai ao encontro da visão adotada neste trabalho. A origem de tais moedas sociais estaria nos clubes de trocas (os quais reúnem produtores-consumidores) e seriam uma alternativa à troca direta. A autora considera que os clubes de trocas brasileiros foram diretamente inspirados nas experiências argentina e canadense, o que remete diretamente ao primeiro *LETS*, surgido no Canadá. Blanc (2011) considera que o Banco Palmas é um sistema típico da terceira geração de moedas complementares, ou seja, um sistema em tudo semelhante ao Hours, tendo notavelmente um viés econômico, ou seja, um viés que vai além do local e do comunitário, e passa pela construção das relações econômicas de produção e consumo (a primeira geração seriam os *LETS*, a segunda os *time banks*). Rigo (2014), entretanto, faz uma ressalva a essa visão. Para a autora, o conceito de "projeto", com base em três definições ideais de moedas, utilizado por Blanc (2011) é limitado para definir totalmente os objetivos dos bancos comunitários no Brasil. Entretanto, para fins das análises a serem conduzidas neste trabalho, não notamos diferenças significativas, em termos técnicos, nas experiências brasileiras, embora elas existam em termos sociais e de orientação filosófica adotadas, não só entre as experiências brasileiras e a americana, mas entre praticamente todas as experiências relatadas por diferentes autores, oriundas de diferentes países. Logo, é apenas possível chegar-se a um denominador comum. Este denominador comum não deve, contudo, ser entendido como algo capaz de definir cada experiência particular de forma completa, mas apenas como um meio de agrupá-las para fins de uma classificação que tem um objetivo bem definido.

O último tipo de experiência notável descrito na literatura são as *CLCs* (*Convertible Local Currencies*), ou Moedas Locais Conversíveis. Blanc (2011) faz um esboço do que para ele viria a ser esta quarta geração de moedas complementares: moedas em que haveria uma grande participação de governos locais. Entretanto, essa visão não encontra paralelo em outros

trabalhos posteriores, haja vista a dinâmica típica do movimento de moedas complementares, portanto, pode-se assumir que Blanc (2011) falhou em sua previsão. Dittmer (2013), divide as moedas complementares em quatro categorias, as três primeiras sendo exatamente equivalentes às três primeiras gerações apontadas por Blanc (2011). A quarta categoria, entretanto, seriam justamente as *CLCs*. Como o próprio nome sugere, o que torna as *CLCs* especialmente distintas é a garantia de sua conversibilidade em moeda estatal, o que significa que o portador da moeda pode exigir a qualquer momento sua conversão em moeda oficial, o que seria equivalente a converter a moeda em seu lastro. Dittmer (2013) sugere que o melhor exemplo de *CLC* seriam os *Regiogelder* da Alemanha, notavelmente o *Chiemgauer*. Um outro exemplo seria o *BerkShare* de *Massachusetts.* Como frisado por Rigo (2014), a total conversibilidade pode ser resultado justamente do apoio ou ao menos do reconhecimento dado pelo Estado a tais iniciativas, o que também facilita a relação com o comércio formal, o qual terá menos barreiras à aceitação da moeda complementar. Entretanto, a intenção de tais moedas ainda é o fomento a uma rede econômica regional, portanto é comum o uso de barreiras à conversão da moeda em seu lastro. Isto ocorre, por exemplo, com o *Chiemgauer*, onde comerciantes sofreriam uma perda de 5% (2% para a manutenção do sistema e 3% como doação para alguma associação regional) ao executar a troca da moeda por euros (VOLKMANN, 2012).

Cabe, por fim, ressaltar que algumas características são comuns a todos os sistemas descritos na literatura. Por exemplo, todas as moedas comunitárias analisadas se caracterizam pela inexistência de juros em seus sistemas, visto não serem moedas bancárias, mas moedas com finalidade tipicamente social, comunitária, de escopo local. A cobrança de juros não só iria contra os princípios sob os quais tais sistemas emergem, como seria ilegal do ponto de vista jurídico, já que as associações responsáveis por administrar essas moedas complementares não são instituições financeiras. Justamente por essas moedas complementares serem experiências à margem do sistema financeiro de uma país é que sua circulação deve ser mantida em "círculos fechados" (*closed loops*), a fim de evitar que tenham efeitos monetários sobre a moeda estatal, como inflação (CAMINHA e FIGUEIREDO, 2011). Uma outra característica comum relevante é a escolha da unidade monetária, a qual é realizada pela comunidade ou pelo criador da moeda complementar como um ato de sua autodeterminação e autonomia. Por exemplo, a existência de qualquer vínculo ou não com a moeda estatal ou com qualquer outra moeda é uma escolha individual de cada sistema de moeda complementar, exceto nos casos das moedas conversíveis, em que necessariamente haverá um vínculo com uma moeda estatal. Por conta disso, Dittmer (2013) considera as *CLCs* um retrocesso quanto ao papel de equilíbrio social e ecológico das

relações econômicas, o qual seria melhor desempenhado pelos sistemas *LETS*, *time banks* e Hours.

O método de classificação adotado neste trabalho emergiu, inicialmente, de forma intuitiva a partir das diferentes experiências relatadas na literatura. O relato de tais experiências foi suficiente para que se chegasse a uma primeira classificação, surgida a partir da comparação das características básicas essenciais de cada modelo de moeda, como a emissão ou não de papel-moeda. Porém, tais características básicas não são sempre absolutas. Volkmann (2012) aponta para o fato de que a maioria das moedas complementares existentes na Alemanha, Suíça e Áustria adotam sistemas de desvalorização da moeda em função do tempo (teoria de oxidação da moeda). Entretanto, esta não é uma característica chave, ou obrigatória, de nenhum dos tipos de moedas descritos por quaisquer dos autores citados anteriormente. Isso colocaria, então, as experiências dos países de língua germânica em uma categoria à parte? Não nos pareceu correto, a esta altura, criar uma nova categoria apenas em função de um item particular, de um caso isolado, porém até então não dispúnhamos de um suporte teórico para tal decisão. Logo, foi necessário recorrer a uma base teórica mais sólida a fim de aperfeiçoar o método de classificação dessas experiências, dessas moedas complementares, em função de suas características individuais. O grande desafio, então, seria definir perfeitamente um conjunto relevante de itens, de características, que definissem um sistema de troca, uma moeda complementar, permitindo alguma variação interna sem, contudo, resultar em um sistema à parte, essencialmente diferente. A esse respeito, os trabalhos de Blanc (2011) e Rigo (2014) foram de suma importância.

Por meio do trabalho de Blanc (2011) foi possível verificar que o método intuitivo inicialmente adotado neste trabalho estava em consonância com as conclusões do *Social Money Workshop Facilitation Committee*, um comitê criado em 2006 com a intenção de explorar a "Tipologia e a Terminologia" até então usadas para descrever os "sistemas de mecanismos de troca" e "delinear uma tipologia comum" que pudesse ser adotada para descrever tais sistemas. (BLANC, 2011). O comitê aponta três conclusões gerais: 1. Há que se distinguir uma tipologia de itens, os quais permitem identificar características particulares, de uma tipologia de sistemas, os quais emergem da combinação relevante dos itens, e não das características particulares ou das variações que cada item pode comportar; 2. Deve-se buscar uma tipologia geral de sistemas monetários, ao invés de uma tipologia específica de moedas complementares, pois estas podem ou não apresentar particularidades que as tornem distintas dos sistemas monetários existentes;

3. Uma tipologia não deve ser construída a fim de classificar observações, mas deve sim ser flexível o suficiente para comportar o surgimento de inovações, ou seja, para abranger experiências não observadas no momento de sua criação (BLANC, 2011).

Blanc (2011) considera que construir uma tipologia comum para abranger todos os casos existentes pode ser um esforço vão, pois diferentes tipologias podem ser propostas em torno de diferentes propósitos bem definidos. Um direcionamento adotado de forma intuitiva neste trabalho, cuja importância se tornou muito mais clara à luz do trabalho de Blanc (2011), é o fato de que a utilidade de uma classificação pode, e frequentemente está, intrinsicamente vinculada a um objetivo claro. Em outras palavras, não é possível eleger uma tipologia para moedas complementares sem que se tenha um propósito bem definido, pois tal tipologia dificilmente será universal e definitiva, ainda que este seja seu propósito. Logo, o conjunto de itens ou o conjunto de características representativas de uma classe específica de moeda complementar será definido aqui em função da análise a ser realizada posteriormente, em que se verificará a adequação das *colored* bitcoins a cada uma dessas classes. Logo, não há dissociação possível entre as categorias de moedas complementares propostas nesta seção e as análises a respeito do Bitcoin apresentadas posteriormente neste trabalho, pois a construção deste conhecimento acontece de forma integrada. Em suma, a perspectiva adotada no ato de eleger a tipologia dos itens utilizados para classificar as moedas complementares já implica um conhecimento prévio das características chave das *colored* bitcoins, contra as quais os sistemas de moedas complementares identificados serão comparados posteriormente. Portanto, há um pressuposto, que é o caráter técnico de cada moeda complementar.

Rigo (2014), a partir de uma discussão extensa de três trabalhos anteriores de Blanc (1998, 2011, 2013), propõe sua própria classificação de moedas complementares, a qual não se relaciona a aspectos técnicos das moedas e seria, portanto, mais uma tipologia do universo de experiências de moedas complementas. Entretanto, a classificação adotada por Rigo (2014) proporciona uma visão diferenciada digna de menção, e a qual também contribuiu imensamente para a classificação proposta neste trabalho. Rigo (2014) define as moedas complementares em função de seis aspectos básicos, os quais se relacionam com seis questões fundamentais a respeito do: onde; por que; por quem; para quem; como e sob qual gestão tais moedas existem. Para fins de nossa análise, os dois aspectos mais importantes serão o "como a moeda funciona?" e o "que atores fazem a gestão da moeda?". Em relação a como tais moedas se constituem: há moedas impressas (Ithaca HOURS, Palmas etc.) e outras apenas virtuais (*LETS, time banks*); há moedas indexadas a uma moeda nacional (todas as moedas dos BCDs brasileiros) e outras

não indexadas ou indexadas a outras unidades de referência, como o tempo (*Time Dollars* e *time banks*) e há moedas com sistemas de oxidação ou desvalorização periódica (*Chiemgauer*). Entretanto, há moedas que mesclam algumas dessas características, por exemplo, fazendo uso de moeda impressa e eletrônica, o que pode ser visto como uma característica natural do ambiente de inovação e experimentação em que tais moedas surgem. Quanto aos aspectos de gestão da moeda, a conclusão é que em todos os sistemas a gestão recai tipicamente sobre uma organização da sociedade civil, a qual fica responsável pelos processos de gestão da circulação (registros contábeis, definição de mecanismos de controle, emissão de moeda etc.). Essa administração pode ser centralizada ou participativa e algumas contam com o apoio de outras instituições, como governos locais, empresas privadas, ONGs etc. Por fim, Rigo (2014) se vale do aspecto "onde a moeda foi criada?" para identificar dois grandes conjuntos distintos: 1) sistemas de trocas, onde estariam incluídos *LETS e time banks*, os quais são marcados pela ênfase no papel do sistema como um meio e facilitador de trocas; 2) projetos com maior comprometimento com o desenvolvimento de territórios, mas que ainda mantém forte ênfase na construção de relações de confiança entre os atores, onde se incluem todas as moedas dos BCDs brasileiros e, por extensão, experiências como o *Ithaca HOURS*.

Portanto, a partir da compilação de todas essas informações colhidas em trabalhos de diferentes autores, chegamos ao seguinte cenário de aspectos técnicos: 1) Existem sistemas de moedas virtuais em que o valor da moeda é meramente simbólico, representativo das relações entre indivíduos, mas nunca equivalente a uma outra moeda ou a um bem material. Se enquadram nessa categoria os LETS, os time banks e qualquer outra experiência de moeda complementar sem lastro; 2) Existem moedas em que há uma moeda física, impressa, onde a conversibilidade em seu lastro, o qual é definido pela comunidade, é parcialmente garantida, porém eminentemente indesejável, pois vai contra os objetivos da moeda, que é criar coesão e desenvolvimento local ou comunitário. Assim, não há garantia da existência de lastro para toda e qualquer cédula emitida. Nessa categoria estão incluídas as moedas dos BCDs brasileiros e o *Ithaca HOURS*; 3) Existem moedas semelhantes às anteriores, porém onde a conversibilidade em seu lastro é perfeitamente garantida, desde que sob determinadas condições, a fim de criar incentivos ao uso direto da moeda complementar pelos recebedores, evitando a conversão em seu lastro. Porém, nestes sistemas, a conversão da moeda é vista como uma parte previsível e natural do sistema, e toda moeda emitida deve portanto estar resguardada em moeda oficial.

Embora existam diversos outros detalhes a serem considerados, os quais serão devidamente elucidados a seguir, consideramos que a divisão das moedas complementares em três categorias, eminentemente em função de seu lastro e sua conversibilidade, é imprescindível à análise conduzida neste trabalho. Isso se dá por dois motivos em particular: 1) essa divisão é condizente com as experiências relatadas na literatura, em que os sistemas de troca do tipo *LETS* e bancos de horas são visivelmente semelhantes, enquanto os sistemas Hours e as moedas conversíveis definitivamente constituem categorias distintas; 2) O Bitcoin é uma tecnologia candidata a moeda, a qual possui uma taxa de câmbio flutuante tipicamente atrelada ao dólar americano. Portanto, ao adotar tal tecnologia para se construir uma moeda complementar, a possibilidade de conversão de bitcoins em dólares se tornaria uma característica (desejável ou não) do sistema. Logo, a existência de lastro, resgatável ou não, nas moedas complementares se torna uma característica chave. Portanto, julgamos que os demais aspectos característicos das experiências relatadas na literatura não justificam a criação de uma classe à parte, porém estes serão devidamente analisados no conjunto das características de cada uma das três classes propostas.

3.2 Comparação das Classes de Moedas Complementares

As tabelas abaixo são fruto da compilação de informações presentes nos trabalhos citados na seção anterior. Buscamos identificar as características técnicas e processos associados a cada tipo de moeda e compara-los lado a lado. Notavelmente, colhemos informações a respeito das características particulares de cada classe aqui definida a partir dos trabalhos de Collom (2005), Collom (2011), Freire (2011), Volkman (2012) e Dittmer (2013). As tabelas abaixo serão de fundamental importância para que possamos discutir, a seguir, a adequação do Bitcoin em cada caso específico. A primeira tabela compara as características gerais de cada sistema de moeda comunitária, sem fazer juízos de valor ou de superioridade entre uma característica e outra, visto que tais moedas frequentemente se dedicam a atingir objetivos consideravelmente distintos. A segunda tabela, entretanto, claramente identifica aquilo que são vulnerabilidades nos sistemas, características de *design* desses sistemas que podem ser exploradas por pessoas mal-intencionadas ou podem conduzir a crises internas no sistema.

Por fim, cabe notar a nomenclatura adotada para as três categorias propostas: 1) A primeira categoria é nomeada Sistemas de Trocas Assíncronas, a fim de enfatizar que o aspecto chave de tais sistemas e sua ênfase no meio de troca. Nesses sistemas, a tecnologia é usada como uma forma de substituir o escambo, ou troca direta, sem que haja tipicamente qualquer preocupação com o desenvolvimento das relações econômicas a nível local ou comunitário. Esses sistemas também se caracterizam fortemente pela ausência de papel-moeda e de lastro em moeda oficial.

Logo, o objetivo maior de tais sistemas é substituir a troca direta, portanto, tornar possível uma troca assíncrona de uma coisa por outra; 2) Decidimos chamar a segunda categoria de Sistemas Hours para manter a fácil identificação com o *Ithaca HOURS*, como um precursor de todas as moedas complementares tipicamente não conversíveis e sem obrigatoriedade de lastro em moeda oficial; 3) A terceira e última categoria é chamada Sistemas de Moedas Conversíveis e, como o próprio nome sugere, esses sistemas se caracterizam por, via de regra, permitirem a total conversão da moeda, a qualquer momento, respeitadas apenas regras de conversão estabelecidas pela comunidade ou pelos gestores do sistema.

Tabela 1 – Características Gerais dos Sistemas de Moedas Complementares

No.	Características Gerais	Sistemas de Trocas Assíncronas	Sistemas Hours	Sistemas de Moedas Conversíveis
1	A unidade monetária é definida pela comunidade	Sim	Sim	Sim
2	Há emissão de papel-moeda	Não	Sim	Sim
3	Há uso de moeda virtual ou eletrônica	Sim (apenas para fins de registro da transação em sistema)	Sim (a critério da comunidade)	Sim (a critério da comunidade)
4	Moeda pode ser convertida em seu lastro (moeda de curso legal ou moeda equivalente)	Não	Não	Sim
5	É necessário guardar registro de todas as transações realizadas	Sim	Não	Não
6	É requerido cadastro prévio para participar do sistema	Sim	Tipicamente Sim	Tipicamente não
7	Pode ser cobrada uma taxa no ato do cadastro do participante	Sim	Sim	Não

8	Pessoas não cadastradas podem receber pagamentos (ou adquirir moeda)	Não	Sim	Sim
9	Ofertas e demandas são cadastradas e publicadas periodicamente	Sim	Não	Não
10	Há votação para deliberar sobre a concessão de empréstimos	Não se aplica	Sim	Não se aplica
11	Pode haver recolhimento de taxas (ou percentuais) no ato de conversão da moeda	Não	Sim	Sim
12	Pode ser aplicado algum método de desvalorização da moeda em função do tempo	Sim	Sim	Sim
13	Volume de transações é ilimitado	Depende da capacidade de se manter registro	Sim	Sim
14	Geração da moeda ocorre somente no ato de realização de uma transação entre os atores	Sim	Não	Sim (ainda que num ato de aquisição da moeda via câmbio)
15	Possibilita a criação relações de troca com a rede de comércio formal	Não	Sim	Sim
16	Moeda complementar pode ser emitida por bancos comerciais	Não	Não	Sim

(COLLOM, 2005), (BLANC, 2011), (FREIRE, 2011), (COLLOM, 2012), (VOLKMANN, 2012), (DITTMER, 2013), (RIGO, 2014)

Tabela 2 – Vulnerabilidades nos Sistemas de Moedas Complementares

No.	Vulnerabilidades	Sistemas de Trocas Assíncronas	Sistemas Hours	Sistemas de Moedas Conversíveis
1	Vulnerável a acumulação excessiva de débitos ou de créditos	Sim (débitos)	Sim (créditos)	Não
2	Volume de transparência contábil requerido cresce na mesma proporção do número de participantes	Sim	Não	Não
3	Vulnerável a especulação desestabilizadora e inflação	Não	Sim	Sim
4	Requer uma administração central para registrar todas as transações, ofertas e demandas	Sim	Não	Não
5	Ocorrem conflitos de definição de preços em função da qualidade do trabalho individual	Sim	Não	Não
6	Deve-se impor limites à aceitação da moeda a fim de evitar acúmulo de crédito (ou limitar a contração de débito) por indivíduo	Sim	Sim	Não

(COLLOM, 2005), (BLANC, 2011), (FREIRE, 2011), (COLLOM, 2012), (VOLKMANN, 2012), (DITTMER, 2013), (RIGO, 2014)

4 O PROTOCOLO BITCOIN E AS BITCOINS COLORIDAS

Entender o que exatamente é o Bitcoin não é uma tarefa trivial, pois o nome Bitcoin esconde um complexo conjunto de *software*, *hardware*, protocolos e pessoas organizadas em torno desta tecnologia, as quais agem com base em princípios e valores próprios que irão se refletir na tecnologia que criam. Primeiramente, o Bitcoin é um *software* livre, de código aberto, mantido por uma comunidade. Portanto, a fonte de informação mais direta que se pode ter provém da *wiki* mantida por tal comunidade e, embora haja bastante conteúdo, não se pode dizer que sua organização seja sistemática, que haja um objetivo de introduzir toda a dinâmica por trás de tal tecnologia a alguém que esteja se iniciando nela, há apenas uma organização típica de uma enciclopédia, em que o relacionamento entre cada componente dessa tecnologia pode não ficar muito claro. Entretanto, a *wiki* oficial do Bitcoin, a *Bitcoin Wiki*, foi de grande utilidade para a elaboração do glossário deste trabalho, onde cada componente principal do protocolo Bitcoin se encontra devidamente definido, bem como para o entendimento de aspectos técnicos extremamente específicos do Bitcoin.

Um segundo motivo pelo qual é difícil compreender o Bitcoin é que não se encontram muitos artigos científicos ou livros com explicações completas e bem organizadas. Além disso, a maioria dos trabalhos existentes, incluindo a *wiki* oficial, estão publicados em inglês. Ou seja, falta conteúdo e o conteúdo disponível não está acessível a todos, apenas àqueles que dominam uma outra língua. Embora o domínio da língua inglesa seja vasto e crescente, não se pode desconsiderar o esforço que um pesquisador terá ao lidar exclusivamente com fontes bibliográficas escritas em outra língua, que não sua língua materna. Esta seção irá, dentre outras coisas, responder algumas das perguntas que surgiram durante a primeira pesquisa exploratória dos principais trabalhos existentes sobre o Bitcoin, tais como: O que exatamente é o Bitcoin em termos de tecnologia? Como funciona? O Bitcoin é confiável do ponto de vista técnico? O Bitcoin veio para ficar ou pode desaparecer de uma hora para outra? Haveria outras alternativas? O Bitcoin é aceito do ponto de vista jurídico? Como o Bitcoin resolve o problema dos micro pagamentos? Essas questões serão fundamentais para as análises posteriores, bem como para que se entenda exatamente como as bitcoins coloridas são criadas em cima da estrutura já existente do protocolo Bitcoin. Como veremos a seguir, o uso das bitcoins coloridas depende não só de fatores técnicos, mas de escolhas que ainda são objeto de discussão dentro da comunidade responsável pelo Bitcoin.

4.1 O Protocolo Bitcoin

4.1.1 Origem do Bitcoin

Como já mencionado anteriormente, o Bitcoin foi criado por Satoshi Nakamoto. Entretanto, não se sabe exatamente quem é ou quem *são* Satoshi Nakamoto. De acordo com o perfil que em 2009 era associado ao Satoshi Nakamoto "original", e que é possivelmente a única fonte "oficial" de informação a respeito desta figura, Nakamoto seria uma pessoa de nacionalidade japonesa, do sexo masculino, de quarenta anos de idade (Satoshi Nakamoto's Page, 2016). No mais, a identidade de Nakamoto é objeto de especulação até a data de publicação deste trabalho e, possivelmente, continuará sendo para sempre. A menção ao Satoshi Nakamoto "original" feita anteriormente se deve ao fato de que o endereço de e-mail utilizado por Nakamoto na época da publicação do Bitcoin certamente já não pertence mais à mesma pessoa, como pode ser inferido pelo incidente ocorrido em 2010, em que aparentemente houve um ataque contra essa conta de e-mail, a qual teria caído nas mãos de *hackers*. Entretanto, a versão mais provável da história é que esse endereço de e-mail tenha sido meramente abandonado pelo autor (ou autores) do Bitcoin após a publicação do *paper*, e que outra pessoa tenha simplesmente reutilizado o endereço após sua expiração (HILL, 2014). Portanto, não só não se sabe quem Nakamoto é, como não se pode sequer confiar em qualquer um que afirme ser tal pessoa, a não ser pela verificação de sua assinatura digital, a qual é conhecida pela comunidade que mantém o Bitcoin. Entretanto, Nakamoto já não mantém qualquer contato com a comunidade que administra o Bitcoin, havendo inclusive especulações de que ele (no caso de sua identidade ser verdadeira, como sendo apenas um indivíduo) teria morrido (satoshin@gmx.com is compromised, 2014). A revista *Wired*, por meio de seu portal na *Internet*, chegou a publicar matérias especulando que Nakamoto seria na verdade um empreendedor australiano. Entretanto, a revista publicou uma retratação posteriormente, pois a informação se mostrou potencialmente falsa (GREENBERG, 2015).

Alguns questionamentos relevantes já podem ser feitos apenas em torno deste fato: a identidade do criador do Bitcoin é realmente relevante para as pessoas que irão usar a tecnologia? Quais são os riscos de se usar um *software* criado por alguém sobre quem nada se sabe de concreto, a respeito de quem não há qualquer evidência que ateste seu caráter? A resposta para tais questionamentos é bastante simples. Primeiramente, pode-se considerar a partir da experiência que o conhecimento da identidade do criador de uma nova tecnologia rapidamente se torna irrelevante tão logo seu invento passe a ser usado por outros, entretanto os efeitos decorrentes

dos princípios e valores que motivaram sua criação podem ainda ser percebidos e investigados independentemente da identidade de seu criador. Não há qualquer preocupação, por exemplo, a respeito da identidade do criador do papel. Há um legado associado às técnicas de fabricação e aos possíveis usos do papel que já foi incorporado a diversas sociedades e já sofreu alterações e melhorias, ao longo dos séculos. Quantas pessoas se questionam diariamente a respeito dos riscos de se usar o papel? Talvez apenas ambientalistas ou pessoas com preocupações ligadas à logística da produção do papel. Assim como o papel é uma tecnologia conhecida, de amplo acesso, o Bitcoin também pode ser plenamente conhecido e monitorado, pois se trada de um *software* de código aberto, mantido por uma comunidade que mantém discussões majoritariamente abertas a respeito das decisões que estão sendo tomadas sobre o futuro desse *software*, o que significa que qualquer pessoa pode, ao menos, inspecionar seu conteúdo. Porém, e quanto aos interesses que tal tecnologia potencialmente representa? O Bitcoin é suficientemente complexo para que se possa supor que seu criador não trabalhou sozinho nesse projeto. Pode ser que Satoshi Nakamoto seja um grupo que representa determinados interesses, quais seriam esses interesses? Seriam verdadeiros os interesses declarados por essa personalidade misteriosa? A esse respeito, há outros meios de inferir quais seriam esses interesses, os quais existem, mesmo sem saber a identidade dos envolvidos, já que o acesso à tecnologia e às discussões da comunidade que trabalha, que constrói e modifica essa tecnologia, estão abertas ao acesso público e até mesmo à participação. Como veremos mais adiante, de fato o Bitcoin não foi totalmente criado por essa figura misteriosa chamada Satoshi Nakamoto, mas pela comunidade que se formou em torno dessa tecnologia, especialmente pelas pessoas que assumiram a liderança dentro de tal comunidade. Portanto, é possível conhecer a tecnologia e suas motivações a partir da comunidade que a administra, que toma decisões a respeito do seu futuro e, principalmente, que adota essa tecnologia e a divulga para que outros a adotem (FARIA, 2016). O engajamento dessa comunidade foi de suma importância para que o Bitcoin se estabelecesse, especialmente depois que Nakamoto abandonou qualquer discussão relacionada ao projeto, logo no ano seguinte de seu lançamento. Portanto, a partir de 2010 outros atores se tornaram os responsáveis pela manutenção dessa tecnologia, os quais não são figuras envoltas em tanto mistério quanto o criador da mesma, como veremos mais adiante no corpo deste trabalho.

Em seu *post* original, Satoshi Nakamoto, a quem nos referimos aqui como sendo a pessoa ou o grupo que na época da publicação do Bitcoin detinha o acesso e administrava o perfil vinculado a uma conta no *website P2P Foundation*, explica de forma bastante sucinta o funcionamento

do Bitcoin, e deixa um *link* para seu *paper* auto publicado com uma explicação mais aprofundada, o qual pode ser obtido na íntegra a partir do endereço *https://bitcoin.org/bitcoin.pdf* e será usado como uma das principais fontes de informação para explicar o Bitcoin enquanto conceito. Citando o *paper* original, o Bitcoin é "um versão de dinheiro eletrônico puramente P2P" (NAKAMOTO, 2009). Portanto, o objetivo primordial do Bitcoin é possibilitar a transferência de dinheiro e a realização de pagamentos eletrônicos de forma independente de qualquer instituição terceira (como bancos). Porque? Qual a necessidade disso? O próprio Nakamoto explicita os porquês em seu *post* original: tudo gira em torno da busca por privacidade. Quando se realiza um pagamento usando um cartão de crédito, a operadora do cartão, a empresa que administra e controla esse serviço, toma ciência de quem são as duas partes envolvidas na transação, de onde elas estão e, possivelmente, de qual produto está sendo comprado ou vendido (NAKAMOTO, 2009). Entretanto, por qual motivo se poderia desejar maior privacidade? Não seria para fins ilícitos? Não necessariamente, ao menos não de um ponto vista multilateral. Da mesma forma que se pode duvidar das intenções do criador (ou criadores) do Bitcoin, poder-se-ia duvidar das intenções dos governos e das instituições bancárias, especialmente quando o indivíduo se sente atacado e ameaçado pelo sistema vigente. Portanto, a crença no valor do anonimato é sem dúvida um dos motivos por trás da criação do Bitcoin, o qual pode ter sua origem ligada, ainda que indiretamente, às discussões da *Cypherpunk Mailing List*, a qual é uma rede distribuída com o objetivo de interligar pessoas de forma anônima para que se discuta livremente temas relacionados a privacidade, criptografia e liberdade *online*. Essa lista surgiu nos no início dos anos 1990 e é aberta a novos participantes (Cypherpunks Mailing List, 2016). Os chamados *cypherpunks* são ativistas cibernéticos, são pessoas que acreditam no uso de *softwares*, protocolos e criptografia como meio de promoção de mudanças sociais e políticas. Um dos participantes da *Cypherpunk Mailing List* veio a se tornar conhecido mundialmente pela publicação de documentos secretos na *Internet* por meio do *website WikiLeaks*: Julian Assange. É fácil inferir que qualquer ativista que se sinta perseguido por pessoas mais poderosas que ele iria desejar o maior nível de proteção possível, e anonimato é, sem dúvida, uma forma de proteção. Portanto, uma tecnologia como o Bitcoin é de grande valor para uma comunidade como a *cypherpunk* (REDMAN, 2015).

4.1.2 Funcionamento do Bitcoin

Nesta seção iremos apresentar em profundidade o funcionamento do protocolo Bitcoin, cobrindo todos os principais elementos que compõem essa tecnologia. Entretanto, é impossível

entender perfeitamente o que é o Bitcoin apenas por meio da leitura do *paper* original de Nakamoto, pois várias perguntas ainda ficam sem resposta e muitas outras surgem, tais como: quanto tempo leva para se processar um pagamento? O Bitcoin é realmente viável como um meio de pagamento em tempo real ou é viável apenas para transações que não envolvem a troca imediata de bens ou serviços? Como exatamente ocorrem as transações no protocolo Bitcoin? Portanto, foi necessário buscar mais fontes de informação a fim de entender perfeitamente como o Bitcoin funciona. Infelizmente, como já frisamos, as fontes oficiais – *en.bitcoin*.it/*wiki* e *bitcoin.org* – contém explicações ora superficiais ora excessivamente técnicas, sem um contexto que facilite a compreensão do Bitcoin. Logo, além do *paper* de Nakamoto, outros trabalhos foram essenciais para a escrita deste capítulo. Para ajudar a responder as questões mais gerais a respeito do Bitcoin, dois artigos científicos foram de suma importância. O primeiro, escrito por Lee *et al.*, publicado em Janeiro de 2015, é um *survey* sobre moedas virtuais; o segundo, escrito por Kim, publicado em Abril de 2015, analisa os precursores do Bitcoin, que são as moedas virtuais de jogos *online*, gerenciadas voluntariamente por indivíduos. Por outro lado, para responder as questões mais técnicas foi necessário ir em busca de tutorias na *Internet*, capazes de mesclar teoria, detalhes técnicos e o contexto de uso. Dois artigos/tutoriais se destacam dos demais neste sentido: "*How the Bitcoin protocol actually works*", escrito por Michael Nielsen em 2013, e "*Bitcoins the hard way: Using the raw bitcoin protocol*", escrito por Ken Shirriff.

Cabe aqui explicar brevemente o nível de confiança que se pode ter nestes artigos/tutoriais publicados exclusivamente na *Internet*. O primeiro artigo, escrito por Michael Nielsen, busca reinventar o Bitcoin, explicando a importância de cada componente da tecnologia. De acordo com a breve biografia de Nielsen na *Wikipedia*, ele é um *PhD* em Física pela universidade do Novo México, nos EUA, escritor e programador. Há indícios de que essa informação seja verdadeira, pois ela é compatível com a biografia introdutória de Nielsen enquanto palestrante em uma das edições do TEDxWaterloo, sob o tema *Open science now*, que, resumidamente, pode ser visto como uma apologia ao compartilhamento de dados científicos na velocidade de um *Twitter*, por meio do uso de ferramentas que permitam a colaboração (NIELSEN, 2011). Por meio do artigo de Nielsen, descobrimos a existência da seção *Research* na *wiki* oficial do Bitcoin, dedicada à compilação de pesquisas científicas (ou pseudocientíficas) tendo o Bitcoin como tema. Embora a maioria dos artigos seja dedicado a questões excessivamente específicas (como mineração) não pertinentes ao escopo deste trabalho, alguns se mostraram úteis e serão referenciados posteriormente. Entretanto, alguns destes artigos não são publicações científicas

propriamente ditas, mas artigos auto publicados por seus autores, o que diminui sua credibilidade. Portanto, cabe ressaltar que os únicos artigos auto publicados por seus autores referenciados neste trabalho são o artigo original de Nakamoto (2009), criador do Bitcoin, e o artigo original de Rosenfeld (2012), criador das *colored coins*, ou *colored bitcoins*, justamente por estes serem os "trabalhos clássicos" e pioneiros dentro da sua temática. O segundo tutorial utilizado neste trabalho foi escrito por Ken Shirriff, sobre quem não foi possível obter informações muito precisas. Como o nome Ken Shirriff é bastante incomum, poucos resultados são retornados a partir de uma busca no *Google*. A partir dos diversos perfis em redes sociais (como *Twitter*, *Google+* e *LinkedIn*), pode-se inferir que Ken Shirriff é um engenheiro que trabalha no Vale do Silício, possivelmente na *Google*, e teria frequentado a Universidade da Califórnia, *Berkeley*. Por fim, o perfil associado a Ken Shirriff no *Google Scholar* retorna 4 citações de índice h e 3 citações de índice i-10, a partir de 2011. Tendo, portanto, esclarecido tais questões, passaremos ao funcionamento do Bitcoin.

Antes de adentrar nos detalhes do funcionamento do Bitcoin, cabe aqui uma breve analogia capaz de elucidar os porquês de o Bitcoin ser da forma que é. Consideremos o seguinte cenário: um cidadão realiza um pagamento em reais a um vendedor de pasteis. O vendedor recebe 5 reais e o comprador recebe o pastel. Após o comprador ter comido o pastel, o que garante ao vendedor que ele receberá algo em troca por aqueles 5 reais? Não estaria o vendedor entregando o pastel ao seu cliente em um ato de pura fé de que aquela cédula de 5 reais comunicará essa troca aos demais brasileiros? Ou seja, aquela cédula comunicará a qualquer outra pessoa que ele tem direito a algo de valor equivalente a 5 reais. Mas quem garante esse direito? Quem garante que este fato, a troca entre o cliente e o vendedor, realmente ocorreu de modo legítimo? Alguém deve garantir que a cédula de 5 reais é verdadeira; que ela deve obrigatoriamente ser aceita por qualquer brasileiro como meio de pagamento e que o cliente não tem direito de tomar o seu dinheiro de volta, seja por força ou por algum outro artifício, após ter recebido e comido o seu pastel. O responsável por garantir tudo isso neste cenário é o Estado brasileiro, com a ajuda dos bancos públicos e privados, instituições auxiliares, como a Casa da Moeda e instituições fiscalizadoras, de poder coercitivo, como a polícia. O Bitcoin, como se propõe a ser moeda, precisa necessariamente dispor de meios de estabelecer essa dinâmica, de garantir que a troca de bens e serviços por dinheiro virtual, que não deixa de ser uma forma de comunicação, deve ser verdadeira e livre de fraudes. Essa correlação entre dinheiro e comunicação deixa explícito porque o uso de criptografia, que nada mais é que uma forma de codificar informação,

é o coração do funcionamento do Bitcoin. Portanto, o que o Bitcoin faz é substituir o uso de cédulas de papel-moeda, o controle contábil dos bancos públicos e privados e a fiscalização do Estado pelo uso de assinaturas digitais e validação em cadeia. Isso significa, a grosso modo, que cada transação que ocorre no Bitcoin é necessariamente reconhecida por todos os participantes da rede de trocas como sendo legítima antes que outra transação possa ocorrer. É como se na prática o vendedor de pasteis tivesse o poder de comunicar a todos os brasileiros que ele acabou de vender um pastel para seu cliente, e isso pudesse ser reconhecido como legítimo por todo mundo, de modo que formalmente todos os brasileiros estariam reconhecendo o direito do vendedor de pasteis a receber algo em troca dos seus 5 reais posteriormente. Fica claro portanto, que o Bitcoin se propõe a substituir as instituições governamentais, fiscais e bancárias enquanto garantidoras do dinheiro, das trocas entre pessoas. Isso sem dúvida elimina um grande custo de se manter o Estado e todas as taxas bancárias que mantém o sistema. Entretanto, este custo recairá sobre a rede que valida as transações no Bitcoin, ou seja, em teoria recairá sobre todos os seus usuários. Na prática, o Bitcoin é uma anarquia, é uma forma de organização comunitária em que não há qualquer controle central, em que todos são responsáveis pelo todo. E, por incrível que pareça, isto funciona. Como isto é possível e quais mecanismos de controle são necessários é o que veremos a seguir.

Primeiramente, consideremos o problema de validar as transações, de reconhece-las como legítimas. Se o nosso cliente do cenário descrito no parágrafo anterior pagasse pelo pastel usando dinheiro eletrônico (cartão de crédito), quem estaria garantindo a legitimidade desta transação seria uma instituição financeira privada, com autorização para operar em território nacional concedida pelo Estado brasileiro. Já sabemos que o Bitcoin dispõe de meios para dispensar autoridades centrais, mas não de dispensar a validação das transações. Na prática, o Bitcoin dispõe de autoridades emergentes para validar as transações, ou seja, qualquer nó da rede, qualquer pessoa, pode decidir contribuir para esta tarefa de validação. Entretanto, esta contribuição tem um custo, o qual já se tornou tão elevado que transformou a validação de transações Bitcoin em um negócio. Atualmente já não é mais economicamente viável para um novo entrante neste "mercado" investir na compra do *hardware* necessário e pagar pela energia elétrica que será consumida para validar transações (VIILUP, 2015). Em suma, até o momento sabemos que o Bitcoin confia nas assinaturas digitais como meio de impedir fraudes, impedir que se crie moeda ilegítima, e que confia em qualquer pessoa interessada, que disponha de recursos de *hardware* e energia elétrica, para validar as transações. A princípio isso pode levar a crer que o Bitcoin estaria criando um mercado de privilegiados, ou seja, delegando poderes

de validação apenas às pessoas, aos nós da rede, que dispõem de mais recursos. Entretanto, isto não é totalmente verdadeiro. A atividade de validar transações na rede Bitcoin é conhecida como mineração. Isso se deve ao fato de que, ao validar transações, a pessoa responsável pelo trabalho recebe um pagamento em *bitcoins*. Esta tarefa de mineração frequentemente ocorre em sistemas colaborativos chamados *pools* de mineração. Isso permite que nós da rede (pessoas) com menor poder computacional (menos capacidade de adquirir *hardware* e pagar pelo consumo de energia elétrica) possam se associar livremente a fim de compartilharem seu poder computacional individual, bem a fim de dividir entre si o pagamento em *bitcoins* recebido como recompensa. Isto, sem dúvida, torna a rede muito mais democrática do que ela seria caso os *pools* não existissem. Cada *pool* de mineração nada mais é que um sistema de gerência de alocação de tarefas de forma distribuída, hospedado em algum servidor, em qualquer país do mundo, administrado por um indivíduo ou por um grupo de indivíduos, que permitem aos sistemas clientes (computadores pessoais) se conectarem a eles por meio da *Internet*, a fim de compartilhar capacidade de processamento de dados, no caso, o processamento de transações Bitcoin. As formas de divisão do trabalho e dos lucros em *pools* de mineração são uma ciência à parte (ciência, pois de fato envolve modelos teóricos e uso de matemática avançada) e isto foge totalmente ao escopo deste trabalho. Entretanto, muitos dos trabalhos referenciados na seção *Research* da *Bitcoin Wiki* tratam deste assunto.

Portanto, agora que já conhecemos a motivação e a dinâmica básica de funcionamento do Bitcoin, podemos investigar mais a fundo como este sistema realmente funciona, a fim de entender posteriormente como é possível criar "moedas paralelas", as *colored bitcoins*, fazendo uso da infraestrutura deste sistema. Veremos a seguir em maiores detalhes como o uso de assinaturas digitais e a validação de operações se entrelaçam de forma inseparável, se tornando o coração do protocolo Bitcoin, a chamada *block chain*, ou cadeia de blocos. Não deve ser surpresa o fato de que o principal problema que surge ao se criar uma moeda virtual é como evitar que dinheiro seja criado do nada, essa possivelmente é uma das primeiras perguntas a surgirem na mente de qualquer pessoa que ouça falar do Bitcoin. Entrentanto, há um outro problema tão ou mais relevante que esse, que é como evitar que um mesmo valor seja gasto mais de uma vez. Voltemos brevemente ao nosso cenário hipotético anterior. O cliente possui uma nota de 5 reais legítima, verdadeira, que de fato lhe pertence. Entretanto, imagine que agora existem dois vendedores de pasteis, os quais são cegos e estão sentados lado a lado. O cliente malicioso pede que cada um dos vendedores (que não podem ver um ao outro) segurem em um

lado de sua cédula de 5 reais como prova de que ele irá pagar pelo pastel. Assim, o cliente recebe dois pasteis, um de cada vendedor. Pasteis recebidos, o cliente solta a cédula de 5 reais, a qual estará nas mãos de ambos os vendedores de pasteis, cada um segurando de um lado. O cliente recebeu a contrapartida (o pastel) de ambos, portanto, quem ficará com os 5 reais? No mundo real este cenário é extremamente improvável, dadas as limitações físicas. Mas no mundo virtual, este se torna o principal problema, ainda mais quando não há uma autoridade central fiscalizando todos os participantes do sistema. De fato, este é precisamente o problema motivador do *design* do Bitcoin. Como eliminar a autoridade central e ao mesmo tempo garantir que as transações (as quais podem ser validadas por qualquer pessoa, como já vimos) não possam ser fraudadas? No mundo real, as empresas gestoras dos serviços de pagamentos eletrônicos (cartões de crédito) ficam responsáveis por reembolsar seus clientes caso uma transação ilegítima ocorra. Entretanto, isso aumenta o custo de processamento das transações e torna impossível os micro pagamentos, pois seria extremamente caro executar diversos processos de reembolso de compras de pequena monta, que mal pagaram os custos de processamento. Esta também é uma preocupação do Bitcoin. Como manter as transações livres de fraude, sem autoridade central validadora e com um custo de processamento tão baixo que uma transação de qualquer valor, até mesmo de centavos, possa ser processada?

A grande solução para este aparente paradoxo proposta pelo Bitcoin, na pessoa de seu suposto criador Satoshi Nakamoto, é usar uma cadeia de assinaturas digitais, ou seja, vincular todas as transações umas às outras de forma irreversível. Isso não só elimina os custos de intermediar disputas a fim de reverter transações (reembolsar uma das partes), pois tal processo se torna desnecessário, já que a assinatura digital valida obrigatoriamente a identidade das partes mas, ao mesmo tempo, impede a fraude da moeda. Todas as transações já realizadas estão vinculadas umas às outras, de modo que se alguém tentar criar dinheiro "do nada" ou tentar gastar um mesmo valor mais de uma vez, esta pessoa (ou grupo de pessoas) terá que alterar todas as transações já ocorridas. Entretanto, imagine que uma pessoa mal intencionada disponha de recursos computacionais vastíssimos. Como evitar, então, que esta pessoa realize operações fraudulentas e valide suas próprias operações? É necessário impor barreiras que dificultem ou, na prática, tornem impossível, ou extremamente improvável, um ataque deste tipo. Uma transação Bitcoin não constitui, por si só, um volume grande de dados a serem validados, chegando ao tamanho máximo de algumas dezenas de *bytes*. Portanto, se torna necessário aumentar de alguma forma a "carga" ou o "peso" computacional das transações a serem validadas. Isto ocorre de duas formas. Primeiramente, as transações devem ser agrupadas em

blocos de até 1MB (1024 *bytes*) a fim de serem validadas em conjunto. Além disso, cada bloco de transações validadas deve vir acompanhado de uma "prova do trabalho executado" ou *proof-of-work*, que nada mais é que a solução para um problema matemático difícil, problema este que exige grande poder computacional e, geralmente, um certo tempo para que possa ser resolvido. Entretanto, falta ainda o componente crucial deste sistema, a *block chain*. Cada bloco validado, acompanhado de sua "prova do trabalho executado" deve ser aceito pela rede P2P, a qual verificará a solução para aquele problema matemático antes de aceita-lo, ou seja, verificará se o *proof-of-work* daquele bloco é, de fato, verdadeiro. Essa tarefa de verificação é trivial, como tipicamente ocorre com problemas matemáticos complexos, onde a resposta correta pode ser facilmente verificada, uma vez que tenha sido encontrada. Após aceito, esse bloco passará a integrar a "cadeia oficial de blocos de transações", a *block chain*, a qual funciona como um livro-razão aberto, o qual registra todas as transações já realizadas em *bitcoins* e está acessível a todos que queiram consulta-lo. Portanto, as transações realizadas em *bitcoins* são agrupadas em blocos, os quais devem passar por um processo de validação que é propositalmente custoso em termos computacionais. Após ser validado por um nó qualquer da rede, esse bloco começa a ser aceito pelos demais nós como sendo válido. Desta forma, o Bitcoin cosegue funcionar de forma independente de uma autoridade central validadora, pois cada nó da rede P2P se torna um "banco" em potencial, capaz de validar as transações e manter registro de todas elas. Entretanto, isso significa que todas as transações realizadas em *bitcoins*, ou seja, tudo que uma pessoa comprar ou vender poderá ser conhecido por todo mundo? E o que ocorre se dois nós da rede validarem um bloco ao mesmo tempo? Quem ficará com o crédito? Quanto tempo leva para essa tarefa de validação ser concluída? Uma pessoa deve, então, esperar pela validação de sua transação antes de entregar um bem ou serviço a outra pessoa em troca de *bitcoins*? Todas essas perguntas serão respondidas de forma satisfatória mais à frente. Elas conduzem à arquitetura interna do Bitcoin, ou seja, aos detalhes técnicos de implementação que fazem com que a teoria por trás do Bitcoin de fato funcione na prática.

Primeiramente, vamos examinar as questões relacionadas à identidade (e ao anonimato) das partes de uma transação. Como já vimos, o anonimato é um princípio do Bitcoin sustentado pela comunidade gestora desta tecnologia. Portanto, a aparente contradição entre uma *block chain* pública e a garantia do anonimato é ilusória, pois este problema é justamente resolvido pelo uso das assinaturas digitais, já mencionadas anteriormente, as quais se baseiam no uso de criptografia de chave pública, uma tecnologia bastante conhecida e estudada no campo das

Redes de Computadores. As assinaturas digitais garantem que as partes de uma transação são legítimas, não permitindo o repúdio às transações realizadas, ou seja, não há espaço para contestação. Uma vez que ambas as partes "assinaram" digitalmente a transação, elas próprias, obrigatoriamente, realizaram essa transação. Entretanto, isso não elimina o risco de furto ou roubo momentâneo de identidade, ou da *wallet* (carteira) de um indivíduo. A carteira (*wallet*) é um arquivo digital (tipicamente *wallet.dat*) padrão do Bitcoin, onde se guarda, dentre outras coisas, o saldo em *bitcoins* e os pares de chaves pública/privada de seus donos, chaves essas que são o componente fundamental das assinaturas digitais. Se uma pessoa mal intencionada roubar a "identidade digital" (a carteira) de outra e gastar suas *bitcoins*, para todos os efeitos foi a pessoa vítima do roubo que realizou as transações. Portanto, é imprescindível que se mantenha a *wallet* o mais protegida possível. Isso pode parecer, a princípio, algo cruel em comparação com o que ocorre com os cartões de crédito. Entretanto, há uma diferença fundamental entre as duas tecnologias. Com o uso de assinaturas digitais, o indivíduo sempre manterá o seu "cartão de crédito" (sua *wallet*, contendo seus pares de chaves públicas e privadas) escondida de todos os demais. Em momento algum o usuário será solicitado a divulgar a natureza (ou os caracteres salvos em arquivo) de sua *wallet*, como ocorre com os cartões de crédito, em que o usuário deve prover todos os detalhes de seu cartão para autorizar uma compra pela *Internet*. Entretanto, há uma outra vantagem no uso de assinaturas digitais, que é a ocultação da identidade real das partes de uma transação. É possível, por exemplo, saber que A enviou um valor de 10 *bitcoins* para B. Porém, não é possível saber quem é A ou quem é B, qual seu nome, ou qualquer outra informação pessoal. Não há qualquer autoridade na rede P2P que tenha meios de saber exatamente quem são as partes. É possível, entretanto, trançar padrões de compra, caso o indivíduo sempre utilize o mesmo par de chaves pública/privada. Entretanto, para impedir até mesmo esta identificação potencial de padrões de compra, o que na prática levaria à identificação da pessoa, a comunidade Bitcoin recomenda que as partes utilizem um par de chaves pública/privada por transação. Isso seria equivalente, a grosso modo, a trocar de cartão de crédito a cada compra realizada pela *Internet*. Portanto, as assinaturas digitais são um componente chave na garantia do anonimato, mas também são elas que atuam no estabelecimento de elos entre todas as transações, a fim de formar a *block chain*. Cabe frisar que a explicação detalhada do funcionamento das assinaturas digitais e da criptografia de chave pública vão além do escopo deste trabalho. Caso o leitor não seja minimamente familiar com esses conceitos, recomendamos a leitura de tais tópicos na *Wikipedia* ou em algum livro de Redes de Computadores.

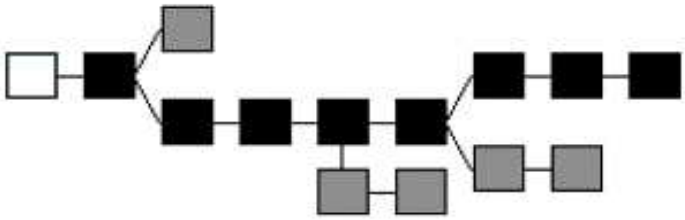
Portanto, tendo entendido como as assinaturas digitais atuam na proteção da identidade das partes de uma transação, veremos a seguir um modelo simplificado de como se estabelece a *block chain*, ou o elo entre blocos de transações. Cabe frisar, brevemente, que o saldo em *bitcoins* é mantido na *wallet* meramente por meio de referências às transações de um usuário. Ou seja, não é mantido um valor numérico que representa o saldo, mas sim a referência a todas as transações de débito e crédito daquele usuário. Portanto, se as transações que conferiram crédito àquele usuário são verdadeiras, o crédito em *bitcoins* daquele usuário também o é. Isso por si só elimina, na prática, a possibilidade de se criar *bitcoins* "do nada", portanto, um vendedor de pasteis poderia aceitar um pagamento em *bitcoins* sem medo de que aquelas *bitcoins* recebidas sejam "falsas". Importa, somente, ter certeza de que a transação será validada pela rede P2P, e isso pode ser parcialmente garantido de imediato (e totalmente garantido após 60 minutos), como explicaremos mais adiante. Entretanto, há serviços de terceiros que "assumem esse risco" para o vendedor, ou seja, um terceiro intermediaria a transação, pagaria imediatamente a importância de 5 reais (reais, não *bitcoins*) ao vendedor de pasteis, cobraria uma pequena taxa por isso, e aguardaria até que a transação fosse validada para receber as *bitcoins*. O prazo médio de validação de uma transação é de 10 minutos, esta é a meta, e isso foi determinado pela comunidade Bitcoin (as razões por trás dessa escolha também serão explicadas mais adiante). Após 10 minutos já começa a ser minimamente garantido que aquela transação será permanentemente aceita pela rede P2P como válida. Entretanto, é perfeitamente plausível aceitar pagamentos de pequeno valor sem depender de terceiros para assumirem riscos, ou sem mesmo aguardar por essa validação, pois já se sabe que, com altíssima probabilidade, se alguém está gastando *bitcoins* é porque elas existem e não estão sendo gastas ao mesmo tempo para pagar a dois ou mais vendedores (especialmente quando o pagamento ocorre "em pessoa" por meio de um telefone celular conectado à *Internet*). Portanto, a utilização de terceiros é mais comum para produtos de alto valor agregado, como ocorre com a empresa *Dell*, que aceita *bitcoins* (por meio de terceiros) como meio de pagamento por seus produtos. Como veremos a seguir, cada transação é verificável no tempo, é possível retraçar a ordem cronológica das transações. Isso, aliado à irreversibilidade das transações (garantida pela *block chain* e pela *proof-of-work*) faz com que o saldo em *bitcoins* seja confiável, portanto é praticamente impossível criar bitcoins "do nada", seria apenas possível gastar uma mesma *bitcoin* em diversos lugares ao mesmo tempo, embora isto seja extremamente difícil de fazer devido à "prova do trabalho executado" (*proof-of-work*), a qual também será explicada em maiores

detalhes mais adiante. Logo, conhecendo o funcionamento da *block chain*, é possível saber quando e o quanto é seguro confiar na perenidade de uma transação realizada.

Vejamos, então, em maiores detalhes como funciona a *block chain*. Como já mencionamos, a *block chain* funciona como um livro-razão que registra todas as transações sequencialmente, agrupadas em blocos de transações. O que é importante notar é que um vendedor (uma pessoa recebendo um pagamento em *bitcoins*) só terá como verificar se, naquele momento de recebimento do pagamento, as *bitcoins*, de fato, pertencem ao seu dono. Caso o cliente tente gastar as *bitcoins* duas vezes (na prática, tente realizar uma transação concorrente com a anterior), sua transação será rejeitada pela rede P2P, pois será possível verificar que elas (as *bitcoins*) já foram gastas anteriormente. Entretanto, imagine que um cliente malicioso consiga pagar a dois vendedores exatamente ao mesmo tempo. Qual transação seria validada primeiro? É em função deste fato, que existem prazos para que uma transação seja validada e níveis de confiança associados a esses prazos. A *block chain* é a cadeia oficial e única de transações. Isso significa que só existe uma *block chain* a qual vai sendo incrementada transação a transação (na prática, bloco a bloco). No protocolo Bitcoin, ambos blocos e transações individuais possuem uma forma de ligação direta com, respectivamente, blocos e transações anteriores. No caso da *block chain*, essa ligação se dá pela aplicação de uma função de *hash* sobre o bloco anterior. Essa função de *hash* será explicada em mais detalhes mais adiante, porém é importante notar que o efeito prático disso é que o bloco atual faz referência ao bloco anterior, formando uma cadeia. Entretanto, essa cadeia admite bifurcações temporárias. Isso é necessário para o caso de dois nós da rede terem validado blocos distintos de transações ao mesmo tempo. Mas isso não estaria somente facilitando o trabalho de alguém que esteja tentando gastar *bitcoins* duas vezes? Sim e não. Cada nó da rede, ao validar um bloco de operações, deve escolher "a melhor cadeia" a ser incrementada, ou seja, escolher dentre dois ou mais ramos qual deve receber o novo bloco recém validado. A regra básica é que a melhor cadeia é simplesmente a mais longa. Portanto, um ataque à rede visando gastar *bitcoins* mais de uma vez só seria bem sucedido se o atacante tiver capacidade computacional grande o suficiente para resolver o problema matemático (o *proof-of-work*) antes que qualquer outro nó o faça e decida, propositalmente, incrementar a cadeia onde se encontra sua transação maliciosa. Nakamoto (2009) apresenta uma explicação pouco formal, baseada em probabilidade, para justificar que, caso um nó da rede possua tamanho poder computacional, seria mais vantajoso validar blocos legítimos e lucrar ganhando *bitcoins*, do que realizar um ataque que comprometeria toda a credibilidade da rede. Este tipo de problema, em que há uma rede com participantes legítimos

e maliciosos, onde é necessário manter tal rede livre de ataques, é conhecido como Acordo Bizantino. Em uma análise bem mais formal que a de Nakamoto (2009), foi verificado que uma rede com poder computacional de pelo menos 2/3 daquele de um atacante seria suficiente para manter o bom funcionamento na maioria dos casos, ou seja, manter a rede livre de ataques visando gasto duplo (*double spending*) de moedas (GARAY, KIAYIAS e LEONARDOS, 2015). Essa primeira estrutura básica, um arquitetura externa da *block chain* se encontra resumida na Figura 1, onde o bloco branco representa o primeiro bloco criado, conhecido como *genesis block*, os blocos pretos são aqueles que integram a *block chain*, e os blocos cinzas são blocos inválidos, criados durante uma bifurcação temporária, os quais para todos os efeitos não fazem parte da *block chain*, pois não integram a cadeia mais longa de transações.

Figura 1 – *Block chain* (visão externa da arquitetura do Bitcoin)



(Block chain, 2016)

Cabe ressaltar, entretanto, que qualquer transação que tenha sido incluída em um bloco inválido, virá a ser incluída em um bloco válido futuramente, caso seja uma transação legítima, pois o cliente Bitcoin (o *software* responsável por executar todos os algoritmos de funcionamento do Bitcoin) irá incluir as transações contidas nos blocos inválidos no *pool* de transações a serem reavaliadas por qualquer nó da rede que esteja validando transações. Por fim, cabe notar que, caso um nó da rede se ausente momentaneamente (esteja desconectado da Internet, ou feche o *software* cliente Bitcoin), ao regressar (ao se conectar novamente) esse nó deverá aceitar a cadeia mais longa como a única *block chain* válida. Portanto, esse nó terá que, obrigatoriamente, confiar no trabalho realizado pela rede. Logo, não é possível criar sua própria *block chain* a fim de fraudar transações. O máximo que um atacante poderia fazer é deter um poder computacional imenso (tendendo a metade do poder computacional da rede Bitcoin) a fim de se ter alta probabilidade de executar um ataque bem sucedido (GARAY, KIAYIAS e LEONARDOS,

2015). Considerando que, como já mencionamos, a validação de transações *bitcoin* já se tornou um negócio não lucrativo para novos entrantes (indivíduos não membros de um *pool* de mineração), o custo de aquisição de *hardware* e do pagamento de energia elétrica dificilmente compensariam o investimento (VIILUP, 2015). Entretanto, pelo menos um ataque bem sucedido deste tipo já ocorreu na rede Bitcoin, no ano de 2013, contra um *site* de apostas pela *Internet*. Caso perdesse a aposta, o apostador tentava reverter a transação e obter suas *bitcoins* de volta. Estima-se que esse atacante tenha obtido um valor equivalente a 1.000 *bitcoins* (na época, equivalentes a 124.000 dólares americanos), e que ele detinha cerca de 30% do poder de processamento da rede Bitcoin (Full Validation, 2016). O site oficial *bitcoin.org* contém informações sobre segurança e também sobre os custos (estimados em *bitcoins*) para que se consiga executar um ataque com sucesso. Por exemplo, um ataque partindo de um atacante que detenha 30% do poder de processamento da rede, como o ocorrido em 2013, custaria menos de 500 BTC (*bitcoins*). Logo, como o atacante teria obtido 1.000 BTC como resultado de seu ataque, é possível que a rede Bitcoin venha a ser usada para executar outros ataques como esse no futuro, os quais, devido ao *design* estritamente *peer-to-peer* da rede, não podem ser evitados (Full Validation, 2016). Tipicamente, a comunidade Bitcoin considera que 6 níveis de validação, ou seja, 6 confirmações para uma transação, é um nível seguro para que alguém recebendo pagamentos em *bitcoins* se mantenha a salvo de ataques como esse. Embora comumente se considere que a partir da primeira validação já há algum nível de confiança. Entretanto, estima-se que aquele atacante que detinha 30% do poder de processamento da rede Bitcoin seria capaz de reverter transações com até mesmo 2 ou 3 níveis de confirmação (Full Validation, 2016).

Antes de explicarmos a arquitetura interna da *block chain*, explicaremos brevemente a questão dos prazos de validação de transações. A decisão de se manter a taxa de validação de transações em torno de 1 bloco de transações a cada 10 minutos (um bloco tipicamente contém entre 1000 e 1500 transações) pode ser considerada uma escolha de *design* arbitrária (Average Number of Transactions per Block, 2016). Como o Bitcoin foi a primeira moeda criptográfica a surgir, estimou-se que a taxa de 1 bloco a cada 10 minutos seria suficiente para: a) evitar o excesso de bifurcações (validações simultâneas de blocos por mais de um nó da rede), prevenindo ataques como o descrito no parágrafo anterior; b) manter o tráfego da rede baixo e c) manter o nível de confiança na validação (dificuldade de se obter um *proof-of-work*) alta o suficiente, para que se possa ter um mínimo de confiança na transação a partir da primeira validação. Vejamos, primeiramente, em mais detalhes como o *proof-of-work* funciona. Por escolha de design de seu criador, o Bitcoin realiza um pagamento de 50 *bitcoins* ao nó responsável pela validação de um

bloco. Esse pagamento é cortado pela metade a cada 210.000 blocos o que, a uma taxa de 1 bloco a cada 10 minutos, dá aproximadamente 4 anos. Desde a criação do Bitcoin (em 2009), essa redução no montante pago pela validação de um bloco já ocorreu uma vez e está em vias de ocorrer novamente em breve (em algum momento no ano de 2017). O nível de dificuldade do problema matemático que deve ser resolvido para que se obtenha o *proof-of-work* é variável e é adaptado a cada 2016 blocos validados (aproximadamente a cada duas semanas) a fim de manter a taxa de validação oscilando em torno de 1 bloco a cada 10 minutos. Isso é possível devido à natureza do *proof-of-work*, o qual nada mais é que um *hash* obtido a partir do bloco de transações, tipicamente usando o SHA-256, que é um dos algoritmos da família SHA-2. O SHA-2 (SHA significa *Secure Hash Algorithm*) é uma família de algoritmos criados pela NSA (*National Security Agency*) que implementam as chamadas funções de espalhamento ou *hash*. Como resultado, o *proof-of-work* é uma cadeia de 256 caracteres alfanuméricos obtida a partir do bloco de transações que se está validando por meio de uma função de *hash*. Entretanto, não é qualquer cadeia de caracteres que pode ser considerada uma *proof-of-work*. O que torna o problema especialmente difícil e, portanto, constitui uma prova de que houve trabalho executado, de que algum tempo foi gasto para que se pudesse chegar à solução do problema, é o alvo (*target*). O alvo é a quantidade sequencial de zeros que deve iniciar a cadeia de 256 caracteres. Por exemplo, se o alvo é 18 isso significa que o nó que esteja validando um bloco de transações precisa obter um *hash* a partir do bloco (arquivo contento informações padrão do protocolo e as transações a serem validadas) tal que a cadeia de 256 caracteres seja iniciada por 18 zeros consecutivos. A dificuldade nada mais é que uma medida comparativa do quão difícil é encontrar uma cadeia de caracteres que satisfaça as condições estabelecidas pelo alvo e, como já explicamos, essa dificuldade é ajustada a cada 2016 blocos validados, ou seja, o alvo é recalculado a fim de se obter uma dificuldade tal que o tempo de validação de um bloco seja de 10 minutos. Isso é feito por meio de estimativas e também constitui uma ciência à parte.

Dada a dificuldade de se obter o *proof-of-work*, a partir de 10 minutos, quando tipicamente se obtém a primeira validação para uma transação, ela já pode começar a ser considerada segura. Entretanto, a comunidade Bitcoin recomenda que se aguarde por seis validações, ou seja, que se aguarde até que 5 blocos sucedam ao bloco onde uma dada transação foi incluída para que se tenha certeza de que a transação é irreversível, haja vista o ataque ocorrido em 2013, mencionado anteriormente. Esse processo leva em média 60 minutos (taxa de 1 bloco a cada 10 minutos), entretanto, como já esclarecemos, o tempo de validação de um bloco se guia por

uma média, não por prazos absolutos. Portanto, não há garantias de que uma transação que ocorra agora será validada em 10 minutos. Ao contrário, algumas transações podem nunca ser validadas e simplesmente serem abandonadas na rede P2P por um longo tempo. Isso frequentemente ocorre com transações que não pagam taxas (*fees*), que é um outro elemento importante da arquitetura do Bitcoin. O pagamento de taxas é opcional, entretanto, muitos nós (ou *pools*) que mineram *bitcoins*, irão ignorar transações que não lhes paguem taxas pela validação, aumentando consideravelmente o prazo para que se obtenha a primeira validação. Isto ocorre devido ao crescente custo de se validar transações Bitcoin. No início, o pagamento pela validação de um bloco (originalmente 50 *bitcoins*, que a valor de hoje seria algo em torno de 20 mil dólares americanos) era suficiente para que os "mineradores" pagassem suas despesas e lucrassem. Entretanto, conforme os anos passam e a recompensa pela validação de um bloco é cortada pela metade (atualmente a recompensa é de 25 *bitcoins*), logo os nós validadores tendem a cobrar taxas como forma alternativa de cobrir seus custos (com *hardware* e energia elétrica). De acordo com o *site bitcoinexchangerate.org*, no dia 28 de Março de 2016, o valor estimado da taxa (*fee*) para que uma transação fosse incluída no próximo bloco seria de 4,5 centavos de dólar americano (ou 10566 *satoshis*) (Recommended Bitcoin Network Transaction Fees, 2016). O *satoshi* é a unidade básica do bitcoin, equivalente a uma fração de $1*10^{-8}$ de uma *bitcoin*. Esse nome foi escolhido pela comunidade em homenagem ao suposto criador da moeda. Portanto, é possível verificar que há, de fato, uma indústria emergente estabelecida em torno do Bitcoin, a qual usa *hardware* específico, otimizado para a tarefa de validar *bitcoins* e consome grandes volumes de energia elétrica a fim de validar transações (VIILUP, 2015).

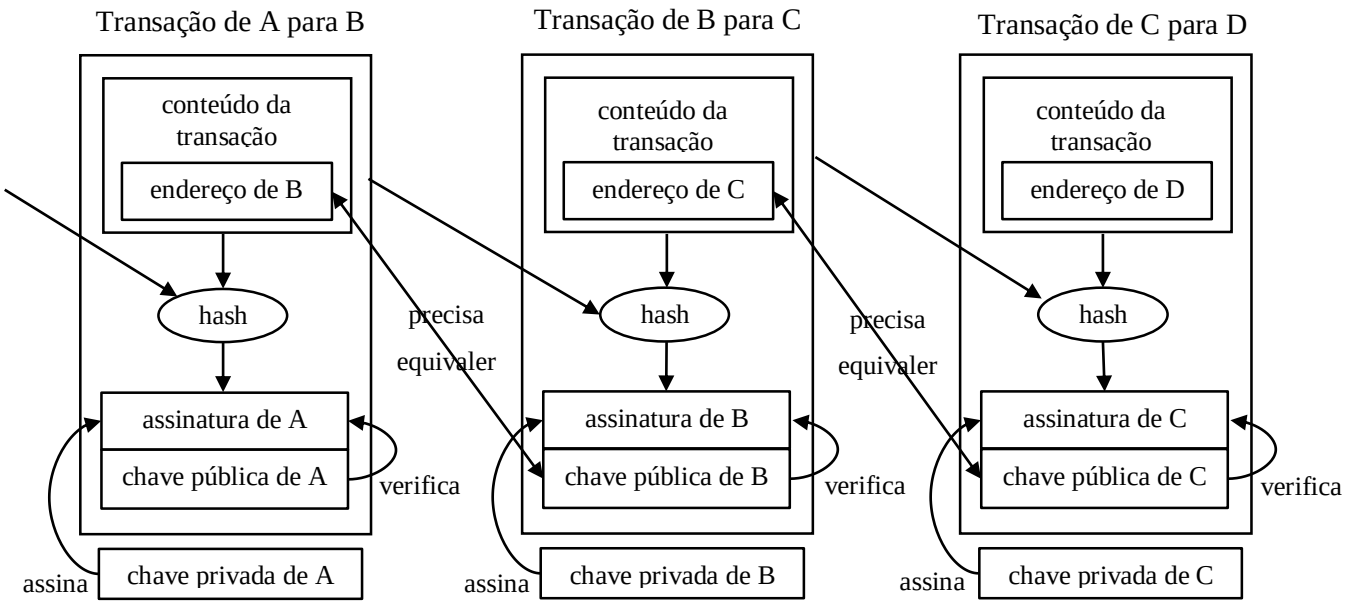
Vejamos agora, então, como todos esses componentes se encaixam na estrutura interna do protocolo Bitcoin. Primeiramente, para que uma pessoa, que chamaremos de "usuário C" (ou somente C) possa usar o Bitcoin é necessário criar uma carteira (*wallet*). Essa carteira conterá um endereço (*address*) que identifica esse usuário de forma única, e conterá pelo menos um par de chaves pública/privada, sendo que o endereço é meramente um *hash* da chave pública, a qual é obtida a partir da chave privada que, por sua vez, é um número hexadecimal aleatório de tamanho 256 *bits*. A geração do endereço e do par de chaves é realizada de forma automatizada pela suíte de aplicativos (*softwares*) que implementam o protocolo Bitcoin, que chamaremos de cliente Bitcoin, ou cliente. Com isso, o usuário C já pode começar a ter *bitcoins* enviadas para seu endereço. Existem diversas implementações de *wallets*, algumas sendo mantidas por instituições terceiras. Entretanto, o modo recomendado de se manter uma *wallet* segura é utilizando o cliente Bitcoin provido pela comunidade Bitcoin, conhecido como *Bitcoin Core*,

que é o menos vulnerável a ataques, ficando sujeito apenas a sofrer ataques do tipo *double spending*, ou reversão de transações, nos casos em que haja baixo nível de validação (menor que 6 níveis) (Full Validation, 2016). Cabe frisar que tanto a chave pública quanto o endereço gerados pelo cliente Bitcoin a partir da chave privada do usuário C serão conhecidos por todos os nós da rede a fim de que eles possam enviar *bitcoins* para C. Entretanto, o processo reverso não é possível, ficando garantida a segurança da chave privada do usuário C. Uma transação em *bitcoins* é composta por *inputs* e *outputs*, ou entradas e saídas. As entradas apontam para saídas de transações anteriores, ou seja, apontam para a origem dos créditos que serão gastos na transação atual. Uma transação pode ter múltiplas saídas, as quais podem ser usadas como "troco". Por exemplo, uma transação que tenha um montante de 2 BTC como entrada pode conferir 1 BTC ao endereço de um vendedor como saída 1 e conferir 1 BTC ao endereço do próprio comprador como saída 2, fazendo com que, na prática, o vendedor receba apenas 1 BTC. Isso necessariamente ocorre desta forma para que se mantenha o elo entre as saídas das transações anteriores e as entradas das transações que as sucedem. No cenário anterior, se a saída 1 conferisse 0.9 BTC ao vendedor e saída 2 conferisse 1 BTC de volta ao comprador, o restante (0.1 BTC) seria transferido ao minerador (nó que vier a validar a transação) como taxa (*fee*). O que torna as transações extremamente complexas, entretanto, é o processo de assinatura das mesmas. Como já sabemos, o Bitcoin utiliza assinaturas digitais, e estas são usadas também como elemento vinculante de uma transação à outra, juntamente com os *inputs* e *outputs*.

Examinemos o cenário em que o usuário C irá receber *bitcoins* do usuário B, chamado de "Transação de B para C". Este cenário se encontra representado na Figura 2. Um *hash* da transação anterior, a qual confere créditos (*bitcoins*) a B será usado como *input* na transação em que B repassa suas *bitcoins* para C, essa transação anterior é chamada "Transação de A para B", em que o usuário A transferiu suas *bitcoins* para B. Além disso, a transação atual (de B para C) irá "envelopar" por meio da função de *hash* outras informações padrão requeridas pelo protocolo Bitcoin para que se forme uma transação. Essas informações são representadas por meio de uma linguagem de *scripting* incluída na suíte Bitcoin, a qual será analisada em maior profundidade no capítulo sobre as Bitcoins Coloridas. Por fim, o cliente Bitcoin irá acrescentar a chave pública de B ao conjunto formado pelo *hash* da transação anterior e pelas informações padrão do protocolo que formam a transação atual. O usuário B, então, irá assinar esse conjunto de informações com sua chave privada. Em resumo, o conjunto formado pela chave pública de B, o *hash* da transação anterior e dos dados da transação atual é chamado de "assinatura de B".

Cabe ressaltar que a chave pública de B deve ser verificada contra o endereço de B da transação anterior, como meio de autorizar o usuário B, como legítimo dono das bitcoins que serão transferidas ao usuário C. Esse processo irá se repetir de forma análoga quando o usuário C quiser transferir suas bitcoins a um usuário D (Transação de C para D). Por fim, após realizar uma transação, o cliente Bitcoin lança essa transação na rede P2P para que seja validada por algum minerador (nó da rede que deseje agrupar transações, produzir uma *proof-of-work* e receber taxas e *bitcoins* geradas pelo protocolo como pagamento).

Figura 2 – Encadeamento de transações (visão interna da arquitetura do Bitcoin)



(SHIRRIFF, 2016)

Cabe, por fim, explicar como os "mineradores" recebem seus pagamentos, ou suas recompensas por bloco "minerado", porém não deve ser surpresa o fato de que esse pagamento ocorre por meio de uma transação. Essa transação especial é gerada pelo protocolo Bitcoin (pela suíte de *softwares* que compõem o protocolo) e produz *bitcoins* "do nada" como forma de pagamento, desde que o minerador tenha produzido, de fato, uma *proof-of-work* válida. O campo *input* desse tipo de transação especial é conhecido como *coinbase*. Isso se deve ao fato de que esse *input* não aponta para a saída de uma transação anterior, pois não há transação anterior nesse caso. Portanto, na prática, o *coinbase* pode conter qualquer informação, pois essa não será usada como *input* propriamente dito para nenhuma transação futura. O *coinbase* do *genesis block* (primeiro bloco da rede Bitcoin, representado pelo bloco branco na *Figura 1*) contém a seguinte informação: "*The Times 03/Jan/2009 Chancellor on brink of second bailout for banks*", que faz

referência à reportagem de capa do jornal *The Times*. Isso foi usado como um meio de provar que nenhuma *bitcoin* existia antes de 03 de Janeiro de 2009. Essas moedas geradas "do nada" possuem um prazo de maturação (*maturation*), o qual determina que elas não podem ser gastas antes que a transação que as gerou tenha recebido 101 confirmações. Essa restrição é muito mais severa que a típica recomendação de se aguardar 6 confirmações para uma transação. Isso ocorre devido à possível existência de blocos inválidos (blocos cinzas da *Figura 1*), os quais, embora apresentem um *proof-of-work* válido, serão futuramente descartados. Portanto, se as *bitcoins* pagas ao minerador daquele bloco que virá a se tornar inválido fossem gastas antes que isso acontecesse, haveria geração imprópria de *bitcoins* na rede, as quais poderiam ser consideradas *bitcoins* "falsas".

Com isso, concluímos as explicações a respeito do protocolo Bitcoin. Não iremos adentrar no nível do conteúdo de cada campo do protocolo, pois isso implicaria uma explicação extensa da linguagem de *scripting* do Bitcoin, o que não só é desnecessário ao escopo deste trabalho como constituiria, possivelmente, um trabalho à parte. Também não adentraremos em maiores especificidades técnicas do protocolo, como tamanho dos campos padrão, pois estas informações, embora sejam muito interessantes, fogem totalmente ao escopo deste trabalho, sendo majoritariamente desnecessárias para que os objetivos propostos sejam alcançados. Faremos, sim, menções à linguagem de *scripting* do Bitcoin naquilo em que importa conhecer para que se entenda o funcionamento da bitcoins coloridas, as quais serão analisadas a seguir, bem como faremos referências ao tamanho (valor máximo em *bytes*) de alguns campos específicos do protocolo naquilo em que importa para o entendimento das bitcoins coloridas.

4.2 Bitcoins Coloridas

O componente da suíte Bitcoin (ou conjunto de *softwares* que implementam o protocolo) que permite a criação das bitcoins coloridas (*colored bitcoins*) é a linguagem de *scripting* integrada ao cliente Bitcoin, ou seja, integrada ao conjunto de *softwares* que, dentre outras coisas, criam, transmitem e validam transações. Essa linguagem permite que se realizem transações bastante complexas, que se tornam verdadeiros "contratos inteligentes". É possível estabelecer condições de validade para uma transação como, por exemplo, estabelecer que uma transação só é válida se apresentar a assinatura de dois dentre três usuários específicos para que possa, então, ser transmitida à rede P2P para se tornar permanente (SHIRRIFF, 2016). É justamente a partir das possibilidades criadas por essa linguagem de *scripting* que Rosenfeld (2012) propõe o arcabouço teórico das *colored coins* (ou *colored bitcoins*). Agora que temos um entendimento

completo de como o Bitcoin funciona, fica claro que não é exatamente uma "*bitcoin*" que será "colorida", mas uma transação que movimenta uma determinada *bitcoin* é que conterá as informações extras, os metadados, chamados de "cores", visto que, na prática, não existem "*bitcoins*", como algo isolado, mas sim transações que as movimentam de um dono para o outro. Portanto, a ação de "colorir" uma moeda *bitcoin* nada mais é que a ação de utilizar alguns códigos específicos desta linguagem de *scripting* a fim de incluir metadados em uma transação. Veremos a seguir o que teoricamente é possível fazer com bitcoins coloridas, como e quais códigos da linguagem de *scripting* são usados para implementar esse conceito, as vantagens e alguns problemas que surgem.

De acordo com Roselfed (2012), o fundamento básico das colored bitcoins é a capacidade de um emissor (um nó da rede Bitcoin) declarar que aquelas bitcoins (ou aquela transação) possui características específicas, especiais, que são representadas sob a forma de metadados, os quais podem fazer sentido apenas para o emissor ou para quem saiba decodifica-los ou atribuir-lhes significados. O trabalho de Rosenfeld (2012) apresenta os possíveis casos de uso para as *colored bitcoins* de maneira bastante informal e, em alguns casos, conceitualmente imprecisa. Interessa aqui, analisar especialmente como o caso de uso relacionado à criação de moedas complementares é apresentado. O autor considera que as colored bitcoins podem ser usadas para a criação de "moedas alternativas" ou "moedas emergentes". Como explicação deste possível caso de uso, Rosenlfed (2012) escreve que: "*A community may want to use a local currency which is similar technically to Bitcoin but detached from it monetarily*". Isso é tudo que o trabalho de Rosenfeld (2012) apresenta a respeito do uso de *colored bitcoins* para fins da criação de uma "moeda alternativa". O autor utiliza os conceitos de comunidade e de moeda local sem apresentar uma definição para os mesmos, o que aliado a interpretações errôneas surgidas na ocasião do lançamento do Bitcoin, as quais especulavam que o Bitcoin seria uma forma de *LETS* (NAKAMOTO, 2009), leva-nos a inferir que o que Rosenfeld (2012) chama de "moeda local" deve ter relação próxima com o que definimos como moedas complementares neste trabalho. Embora, em sentido estrito, pudéssemos considerar que o trabalho de Rosenfeld (2012) só considera as moedas estritamente locais, definidas por sua atuação em um território geopolítico. A seção da *Bitcoin Wiki* que trata da emissão de moedas complementares usando as bitcoins coloridas é tão curta que pode ser transcrita aqui na íntegra: "*A community. e.g. a town, can issue it's own Currency*". Isso dá a entender que a comunidade Bitcoin, ou seja, as pessoas engajadas em manter o código da suíte de softwares que é o Bitcoin, bem como de escrever os artigos da *Bitcoin Wiki*, não possuem vastos conhecimentos a respeito do que são

moedas locais, comunitárias, sociais ou complementares. Diante da ausência de outros trabalhos que venham a esclarecer este ponto, em que pese que nem mesmo o trabalho de Rosenfeld (2012) sobre as *colored bitcoins* se encontra referenciado na seção *Research* da *Bitcoin Wiki*, embora outros dois trabalhos do autor estejam, só nos resta analisar se esse caso de uso para as bitcoins coloridas é realmente possível. Será, portanto, necessário analisar esse possível caso de uso, das *colored bitcoins* como moedas locais, a partir do escopo mais amplo, de todas as possíveis formas de moedas complementares, isto é precisamente o que será feito na próxima, e última, seção deste trabalho.

Na seção anterior deste trabalho, a respeito do funcionamento do Bitcoin, foi dito que os dados de uma transação são representados por meio de uma linguagem de *scripting*. Porém, mais do que isso, há um pequeno programa, um *script*, dentro de cada transação que decide se uma transação é válida ou não. Na prática, cada transação realizada contém em si mesma as regras que definem o que será exigido da próxima transação para esta seja válida, ou seja, a transação anterior, de onde provém o *input* da transação atual determina as regras para que se possa gastar as *bitcoins* recebidas. O script da transação precedente é chamado *scriptPubKey*, já o script da transação atual é chamado *scriptSig*. O mínimo que se exige, por padrão, é que o recebedor das *bitcoins* apresente uma chave pública que produza o mesmo endereço da transação anterior e uma assinatura digital, uma comprovação de que essa pessoa é detentora da chave privada a partir da qual a chave pública foi gerada (esses elementos foram devidamente explicados na seção anterior, vide Figura 2). Entretanto, é possível exigir mais de uma chave ou mesmo nenhuma chave. Essa linguagem de *scripting* do Bitcoin, chamada Script, contém diversas palavras reservadas conhecidas como *opcodes* e funciona de forma semelhante à linguagem Forth, que é uma linguagem baseada em pilha, algo típico de linguagens *assembly*. Como qualquer linguagem, novas palavras reservadas podem ser criadas e outras palavras existentes anteriormente podem ser abolidas. Portanto, a linguagem Script pode sofrer e já sofreu alterações ao longo do tempo (Script, 2016). Não cabe no escopo deste trabalho realizar uma análise aprofundada desta linguagem, portanto examinaremos apenas os *opcodes* relevantes para o entendimento das *colored bitcoins*.

O nome Bitcoins Coloridas (*Colored Coins* ou *Colored Bitcoins*) vem originalmente de uma das formas de se implementar o conceito, chamada EPOBC, a qual fazia uso do *satoshi* (unidade monetária do Bitcoin) como forma de guardar metadados. Portanto, tais metadados ficavam associados a uma *bitcoin*, a um *satoshi*, o qual estaria "colorido". Entretanto, existem outras

alternativas que não implicam no vínculo dos metadados a um *satoshi* dentro do *script* de uma transação. A alternativa mais popular ao EPOBC é conhecida como *Coloring Scheme*, e faz uso do *opcode* OP_RETURN, ao invés do *satoshi*, como forma básica de representar metadados na *block chain* do Bitcoin (Colored Coins, 2016). As demais alternativas existentes são evoluções desse conceito e se dedicam a propósitos mais amplos, à representação de outras formas de metadados que não são objeto de estudo neste trabalho. Para fazer isso, entretanto, precisaremos conhecer ainda um pouco mais sobre como cada uma das duas soluções existentes (EPOBC e *Coloring Schemes*) funcionam. Vejamos portanto, como cada uma funciona.

A principal diferença entre as duas soluções é a sobrecarga que elas causam na rede Bitcoin. Enquanto a solução do tipo *Coloring Schemes* acrescenta uma sobrecarga de dados a cada transação, por meio da inclusão do *opcode* OP_RETURN, o qual não estaria originalmente presente em uma transação, a solução EPOBC faz uso apenas de campos e comandos que já estariam presentes no protocolo, mas que não seriam de outra forma utilizados. O EPOBC utiliza o campo *nSequence* do *input* de uma transação para marcar a transação como "uma transação envolvendo *bitcoins* coloridas", diferenciando esta transação das demais. Este campo também é usado para guardar outras informações relevantes para os algoritmos do EPOBC, que permitirão representar "cores" por meio pares (cor, valor), onde a cor é um *hash* de uma transação geradora (transação que cria essa cor) e o valor é um inteiro representado por meio de *bitcoins*, daí a necessidade de se utilizar pelo menos 1 *satoshi*. Entretanto, é comum utilizar mais que isso, pois como já vimos, há frequentemente a necessidade de se pagar taxas para que as transações sejam processadas, as quais chegam facilmente a 10.000 *satoshis* (Recommended Bitcoin Network Transaction Fees, 2016). Outra característica do EPOBC é que se uma *bitcoin* colorida foi utilizada em outra transação que não seja marcada como "colorida", sua cor será perdida. Já as soluções do tipo *Colored Schemes*, utilizam o *opcode* OP_RETURN, o qual é destinado originalmente a marcar o *output* da transação atual como inválido. Ou seja, na prática, a informação associada ao OP_RETURN não será considerada uma *bitcoin*, portanto não poderá ser gasta, será apenas uma informação extra adicionada à rede *bitcoin*. Entretanto, para que esta transação seja processada, será também necessário incluir algumas *bitcoins* a título de taxas a serem pagas. O uso de OP_RETURN para incluir metadados na rede Bitcoin é objeto de discussão na comunidade Bitcoin. Comprova este fato, a proposta (aprovada pela comunidade) de redução da quantidade de informação que poderia ser incluída via OP_RETURN de 80 *bytes* para 40 *bytes*. Além disso, é permitido o uso de apenas um OP_RETURN por transação (ALMEL e NAYUKI, 2015). Assim como no caso do EPOBC,

torna-se necessário o uso de *softwares* que implementem os algoritmos necessários para a emissão correta de moedas coloridas, bem como para sua posterior identificação e manipulação, caso contrário, os metadados inseridos na rede Bitcoin podem ser para sempre perdidos. Dentre os projetos com base em EPOBC, destacam-se uma *API* escrita em JavaScript e uma implementação de *wallet* para *colored bitcoins* chamada *Cuber*, que é mantida por um banco sediado na Estônia, chamado LHV. Já dentre os projetos que utilizam o paradigma *Colored Schemes*, destaca-se o *Colu*, que provê um aplicativo para telefones celulares, bem como ferramentas de desenvolvimento por meio de uma *API*, que permitiria a criação e gestão de moedas coloridas (Colored Coins, 2016), (Learn, 2016). Portanto, podemos concluir que o uso de *colored bitcoins* encontra-se em um processo recente de estabelecimento e de evolução dentro da comunidade Bitcoin. Há basicamente duas escolhas entre paradigmas, um que não é objeto de conflitos dentro da comunidade, porém é mais vulnerável à perda dos metadados, e outro que é mais robusto, mas enfrenta certa resistência na comunidade. Ambas abordagens não dispensam o desenvolvimento de software específico para lidar com as *colored bitcoins*, os quais se encontram disponíveis como produtos de terceiros (sujeitos a maiores riscos de segurança) ou podem ser criados por meio de *APIs* já dispoíveis.

5 BITCOINS COLORIDAS COMO UMA MOEDA COMPLEMENTAR

5.1 Aspectos Técnicos

A primeira vantagem evidente ao se pensar em adotar bitcoins coloridas como moeda complementar é o volume de dinheiro eletrônico (ou virtual) que se pode criar com poucas, ou mesmo com apenas uma *bitcoin*. A unidade básica do Bitcoin, como já visto anteriormente, é o *satoshi*, que é equivalente a um décimo de milionésimo de uma *bitcoin* (10^{-8} *bitcoin*, ou 0,00000001 BTC). Em valores atuais, na data de publicação deste trabalho, 1 BTC custa em torno de 400 dólares americanos (aproximadamente 1500 reais), o que é um valor extremamente baixo se comparado ao custo de se emitir cédulas em um valor total equivalente a 10 milhões em papel-moeda confiável, com mecanismos mínimos de segurança que dificultem a fraude. A emissão de 102.604 Palmas na implementação da moeda de mesmo nome no Conjunto Palmeiras custou cerca de 51 mil reais no final dos anos noventa (CAMINHA e FIGUEIREDO, 2011). Além disso, toda a economia do Ithaca HOURS, desde a sua fundação no início dos anos 1990 até meados dos anos 2000, requereu a emissão de papel-moeda equivalente a pouco mais de 100 mil USD, o que, considerando que 1 Ithaca HOUR é equivalente a 10 dólares americanos, se traduz em aproximadamente 10 mil Ithaca HOURS em papel-moeda (COLLOM, 2005), volume 100 vezes menor em ordem de grandeza que o volume de dinheiro virtual que poderia ser criado, ou emulado, usando apenas 1 *bitcoin*. Portanto, pode parecer uma ideia muito tentadora, a princípio, utilizar *bitcoins* como substitutas para o papel-moeda, operando, assim, um sistema de moeda complementar totalmente baseado em dinheiro virtual.

Entretanto, ao adotar o Bitcoin como moeda complementar, todas as transações ficariam restritas ao uso de computadores, de telefones celulares capazes de executar aplicativos e da *Internet*, pois embora existam as *paper wallets* (*wallets* impressas em papel) - as quais funcionam de forma análoga ao papel-moeda - seu uso não é recomendado pela comunidade Bitcoin, devido à exposição da chave privada, a qual se encontra impressa na cédula. Excetuam-se os casos de uso em que o objetivo é dar presentes, gorjetas ou realizar o depósito da *paper wallet* em um cofre como meio de mantê-la segura de ataques de *hackers* (Paper Wallet, 2016). Embora as carteiras em papel (*paper wallets*) utilizem mecanismos de segurança semelhantes ao do papel-moeda para dificultar a identificação das informações impressas na cédula, especialmente da chave privada, os riscos de roubo de *bitcoins* são muito maiores, já que bastaria, em alguns casos, obter uma foto da cédula para usar as *bitcoins* (Paper Wallet, 2016). Além disso, no caso de adoção de *paper wallets*, a vantagem anteriormente identificada seria parcialmente perdida, pois haveria um custo de impressão de "papel-moeda". Uma outra

desvantagem reside no fato de que as transações realizadas via *paper wallet* necessariamente deverão ser lançadas na rede P2P do Bitcoin por meio de um computador (ou qualquer dispositivo de *hardware* que possa executar o cliente Bitcoin) posteriormente. Portanto, o acesso a computadores (ou similares) e à *Internet* torna-se imprescindível, o que pode ser difícil em comunidades extremamente pobres que estejam criando uma moeda complementar, implicando em um custo extra de infraestrutura inicial. No Brasil, de acordo com a Pesquisa Nacional por Amostra de Domicílios mais recente (PNAD, 2013, tabela 7.7), 90% dos domicílios com renda de até 10 salários mínimos tinham pelo menos um telefone celular. Entretanto, mesmo que os participantes de uma comunidade onde existe (ou onde se deseje criar) uma moeda complementar possuam telefones celulares, isso não significa que sejam *smartphones* (capazes de executar aplicativos), nem significa que os integrantes de tal comunidade tenham facilidade em manusear o aparelho ou em usar tecnologias virtuais, como aplicativos voltados ao processamento de pagamentos em *bitcoins*. Portanto, haveria no mínimo a necessidade de ensinar os membros daquela comunidade a lidarem com o Bitcoin, passando pelas noções de proteção da *wallet* e pelo uso de ferramentas digitais para processamento de pagamentos, para que só então a comunidade pudesse efetivamente adotar o Bitcoin como base de sua moeda complementar.

Uma outra dificuldade técnica em potencial, seria a escolha da implementação de *colored bitcoins* a ser usada, as quais, de um modo ou de outro, são dependentes do Bitcoin, e isso implica em custos e comprometimentos (*trade-offs*). Como vimos, existem dois paradigmas, o EPOBC e o *Colored Schemes*. Ambos possuem soluções implementadas por terceiros, as quais sempre serão menos confiáveis que o *Bitcoin Core* (o *software* cliente oficial Bitcoin). A única alternativa seria dispor de desenvolvedores para estudarem as APIs do EPOBC e do *Colored Schemes* e desenvolver suas próprias *wallets*, capazes de criar e de gerenciar as *colored bitcoins* enquanto moedas complementares, o que sem dúvida representaria um custo (em horas de trabalho) considerável. Além disso, em ambos os casos existiria a cobrança da taxas para processamento das transações. Como vimos anteriormente, essas taxas facilmente chegam à ordem de 10.000 *satoshis*, Logo, na prática, o volume de dinheiro gerado a partir de 1 BTC deveria cair para algo em torno de 1.000 *colored coins* (cada *colored coin* utilizando em torno de 10.000 *satoshis* a título de taxas). Caso, se desejasse, por exemplo, ter o volume de dinheiro circulante no sistema Ithaca HOURS (10 mil HOURS), seriam necessárias 10 BTC, ao custo de aproximadamente 40 mil dólares (aproximadamente 150 mil reais). Caso se desejasse ter

cerca de 100 mil Palmas, o custo subiria para 1,5 milhão de reais (já que seriam necessárias 100 BTC), um valor absurdamente superior ao custo de se emitir papel-moeda (vide comparação anterior com o valor gasto na época). Portanto, o uso de *colored bitcoins* deveria ser restrito a pequenos sistemas, onde é necessário a emissão de poucas unidades monetárias. Por exemplo, em um sistema em que fossem necessárias apenas 100 unidades monetárias (logo, 100 *colored bitcoins*), seria necessário adquirir 0,1 BTC, ao custo aproximado de 150 reais.

Um outro problema técnico presente na arquitetura do Bitcoin é o limite de processamento de transações por segundo. O Bitcoin consegue processar no máximo 7 transações por segundo, um número extremamente inexpressivo quando comparado à capacidade que a operadora de cartões de crédito Visa possui. A operadora processa em média 2.000 transações por segundo (SIMONITE, 2016) e seria capaz de processar um volume da ordem de dezenas de milhares de transações por segundo (SIMONITE, 2015), acima de 56.000 transações por segundo, de acordo com a empresa (SIMONITE, 2016). Essa limitação do Bitcoin é decorrente do tamanho máximo que um bloco de transações pode ter (1MB), uma decisão de *design* aparentemente arbitrária, a qual é objeto de discussão na comunidade Bitcoin (Block size limit controversy, 2016). Esse problema dificilmente traria um impacto às moedas complementares de forma isolada, pois é um problema do Bitcoin como um todo. Entretanto, como pelo uso de *colored bitcoins* tais moedas complementares estariam utilizando a rede Bitcoin para obter validação de suas transações, ao se atingir o limite de capacidade de processamento, apenas as transações que pagam valores maiores que 10.000 *satoshis* teriam prioridade no seu processamento, levando as demais transações a serem esquecidas na rede P2P. Esse problema se tornou bastante real em Março de 2016, quanto o Bitcoin atingiu o seu limite de processamento por alguns dias e transações começaram a ser “perdidas” na rede. Em um dado momento durante a crise havia mais de 20.000 transações aguardando processamento (SIMONITE, 2016). De acordo com Simonite (2016), durante o incidente o valor da taxa (*fee*) capaz de colocar uma transação na frete da fila de processamento seria da ordem de 7 centavos de dólar (USD), algo em torno de 16.000 *satoshis*. Portanto, caso uma implementação de moeda complementar desejasse contar com esses imprevistos na rede do Bitcoin, seria necessário manter um estoque ocioso de *bitcoins* capazes de serem usadas para pagamentos de taxas, o que só aumentaria os custos de se adotar a tecnologia. Logo, o problema do limite de 7 transações por segundo poderia comprometer momentaneamente o funcionamento de uma moeda complementar que dependesse exclusivamente do Bitcoin.

Como último agravante dos problemas técnicos, Gavin Andersen, que foi coordenador-chefe do código do Bitcoin desde o sumiço de Nakamoto (em 2010) até meados de 2014, lançou em 2015 uma versão alternativa do Bitcoin, o *BitcoinXT* e convidou toda a comunidade Bitcoin a migrar para o seu sistema, a fim de resolver o limite de tamanho de 1 *megabyte* por bloco de transações (SIMONITE, 2015). Diferentemente de Nakamoto, Andersen é uma figura pública, e tem seu rosto conhecido pelo grande público. Entretanto, a necessidade de criar um chamado *fork*, ou bifurcação no código do Bitcoin é bastante real, pois, por questões de *design* do Bitcoin e da *block chain*, o limite de tamanho dos blocos não pode ser resolvido de outra forma senão pelo abandono da implementação atual do Bitcoin e consequente adoção de uma nova suíte de aplicativos, ou seja, um *fork* (Block size limit controversy, 2016). O *BitcoinXT* é em tudo o mais igual ao *Bitcoin Core*, a suíte original. A necessidade de se criar um *fork* do *Bitcoin Core* é um fato conhecido dentro da comunidade Bitcoin e Andersen alega ter adotado a medida provocativa de abandonar o Bitcoin e dar suporte a uma versão paralela do *Bitcoin Core* como meio de acelerar a resolução desse problema crítico (SIMONITE, 2015). No momento, a maioria dos nós da rede Bitcoin ainda utiliza o chamado *Bitcoin Core*, devido a discordâncias quanto aos efeitos negativos que o aumento do tamanho dos blocos acarretaria. Por exemplo, um aumento no tamanho máximo do bloco exigiria, de imediato, mais capacidade de processamento por parte dos mineradores e, como já vimos anteriormente, a questão da viabilidade econômica da atividade de mineração é um aspecto crítico do Bitcoin. Como a atividade de mineração atingiu proporções de uma indústria, havendo empresas constituídas exclusivamente em torno da atividade de mineração de *bitcoins*, fica evidente que há um impasse dentro da comunidade Bitcoin (VIILUP, 2015). Até o momento, o problema do limite de processamento de transações do Bitcoin permanece. Portanto, qualquer implementação de moeda complementar que pretenda utilizar o Bitcoin como base única de funcionamento deve estar ciente dos riscos associados, bem como da ausência de protagonismo que a comunidade responsável por essa moeda complementar teria no que diz respeito às decisões de *design* tomadas pela comunidade Bitcoin.

5.2 Aspectos Jurídico-econômicos

Cabe nesta seção retomar brevemente as características essenciais de uma moeda moderna (moedas atualmente em uso pelos Estados nacionais), identificadas previamente neste trabalho a fim de verificar se as *colored bitcoins* atenderiam a todas ou a algumas dessas características. Os três primeiros aspectos são eminentemente jurídicos, enquanto os três últimos são

eminentemente econômicos: curso legal, curso forçado, poder liberatório, padrão de valor, meio de troca, estoque de riqueza. Como veremos, dentre estes seis aspectos, as *colored bitcoins* atendem apenas aos aspectos eminentemente econômicos, mesmo assim sob determinadas condições, o que já aponta para o não reconhecimento jurídico do Bitcoin enquanto moeda. Exploraremos estas questões em mais detalhes a seguir.

O Bitcoin definitivamente funciona como um meio de troca, esta é a característica fundamental desta tecnologia, pois ela é aceita pela comunidade que a usa e cumpre a função de intermediária nas trocas. Entretanto, uma das características do Bitcoin passível de maior crítica é a alta volatilidade do preço de mercado da moeda, especialmente devido à alta especulação. Isso lança por terra a força do Bitcoin enquanto padrão de valor e enquanto estoque de riqueza. De acordo com o *site coinmarketcap.com*, a cotação do Bitcoin (BTC) saiu do patamar de 150 USD em Outubro de 2013 para atingir 1000 USD por *bitcoin* em Novembro de 2013 despencando, no mês seguinte, para 700 USD/BTC. Atualmente, em Fevereiro de 2016, 1 BTC está valendo cerca de 400 dólares americanos (Bitcoin Charts, 2016). Quanto aos aspectos jurídicos, como o Bitcoin não é moeda nacional em nenhuma nação, não cabem extensas considerações a respeito do curso forçado da moeda, embora, como o Bitcoin não é uma moeda lastreada em qualquer bem tangível, teoricamente o seria uma moeda de curso forçado, caso ela tivesse validade jurídica. Entretanto, a falta de curso legal é o maior ponto fraco do Bitcoin, pois isso significa que sua aceitação como forma de pagamento não é garantida por lei em nenhum país. Desta forma, qualquer pessoa pode se negar a receber pagamentos em *bitcoins* e, já que nenhum Estado aceita (recebe) *bitcoins* como forma de pagamento, não há qualquer possiblidade de o Bitcoin ter poder liberatório. Em parecer dado no ano de 2014, o Serviço de Receita Interna americano (IRS na sigla em inglês) definiu o Bitcoin como *propriedade* para fins de declaração de renda, não como moeda (LEE et al., 2015). Entendimento semelhante é adotado no Brasil pela Receita Federal (ZAMPIERI, 2015). Portanto, caso uma moeda complementar conversível desejasse considerar o Bitcoin como seu lastro, ou meramente como seu meio de troca exclusivo, haveria diversos problemas jurídicos que o impediriam ou pelo menos dificultariam sobremaneira tal tarefa, a depender do tipo de moeda complementar que se deseja criar, visto que o Bitcoin, na melhor das hipóteses, é uma tecnologia que funciona como meio de pagamento e possui um valor de mercado bem definido e flutuante, mas não é uma moeda para todos os efeitos jurídicos e econômicos. Logo, apenas moedas virtuais, como as dos Sistemas de Trocas Assíncronas, as quais não possuem necessariamente qualquer vínculo com moedas oficiais sofreriam menor impacto em função da natureza jurídica do Bitcoin.

Por fim, verifiquemos brevemente os possíveis impactos de uma estabilidade futura no valor do Bitcoin. Kim (2015) analisa o Bitcoin sob dois aspectos alvos de críticas frequentes: a alta volatilidade do preço de mercado da moeda e a ambiguidade dos custos por transação. O autor compara o Bitcoin a moedas virtuais de jogos multijogador *online* (*MMORPGs*) e traça previsões de estabilização do valor do Bitcoin com base na estabilidade do valor dessas moedas de jogos *online*, as quais existem há muito mais tempo que o Bitcoin, chegando a mais de uma década de existência em alguns casos (KIM, 2015). A aquisição de moedas em *MMORPGs* se dá tipicamente por meio da conversão de uma moeda real (moeda oficial, não virtual), por exemplo o dólar americano, em moeda virtual, a qual será usada dentro do ambiente do jogo para qualquer transação que envolva compra de itens digitais, como armas, armaduras e roupas para personagens do jogo. Essas moedas virtuais usadas em jogos eletrônicos são tipicamente adquiridas por meio da compra e, posteriormente, podem ser reconvertidas em moedas de uso corrente, segundo uma taxa de conversão ditada pelo mercado. Outra característica das moedas usadas em jogos eletrônicos é que estas moedas também podem ser geradas a partir do cumprimento de certas condições dentro do universo do jogo. Por exemplo, ao completar uma determinada tarefa, ou ao derrotar determinado inimigo, o jogador poderia receber algumas unidades da moeda virtual usada no universo do jogo (KIM, 2015). Essas características, de fato, são semelhantes às da moeda *bitcoin*, a qual pode ser adquirida por meio da compra (conversão cambial), mas também pode ser adquirida por meio da realização de uma tarefa, qual seja, a validação de blocos de transações. Kim (2015) conclui, a partir da estabilidade apresentada por moedas de *MMORPGs*, que o Bitcoin pode se tornar uma moeda mais estável no futuro. As moedas utilizadas em jogos virtuais analisadas por Kim (2015), as quais apresentavam instabilidade similar à do Bitcoin nos seus primórdios, após uma década de maturação passaram a apresentar volatilidade de um terço daquela do Bitcoin, o que é um nível de volatilidade de valor de mercado similar ao do ouro. Caso essa previsão de estabilidade se confirme, poderia o Bitcoin pode vir a adquirir validade jurídica como moeda em algum país ou território? Nenhuma moeda utilizada em jogos virtuais se propõe a ter a validade jurídica que o Bitcoin almeja. Portanto, a caracterização jurídica do Bitcoin como moeda é incerta e improvável em um futuro próximo (LEE, LONG, *et al.*, 2015). Logo, uma moeda complementar que pretenda utilizar *colored bitcoins* como infraestrutura não poderá depender da validade jurídica do Bitcoin.

5.3 Características Comparadas

Nesta seção, retomaremos as três categorias de moedas complementares identificadas previamente para fins de comparação com as *colored bitcoins*. As discussões desta seção encontram-se resumidas na Tabela 3, a qual provê respostas afirmativas ou negativas para os mesmos aspectos identificados anteriormente na Tabela 1, porém quando se avalia as bitcoins coloridas como meio circulante nos sistemas de moedas complementares. Em alguns casos, os aspectos identificados (características) não serão afetados pelo uso de bitcoins coloridas, o que significa que a adoção dessa tecnologia não interfere, não traz melhorias nem causa transtornos, mas mantém a característica do sistema original intacta. Nestes casos, identificados na tabela como "a critério do sistema original", não faremos maiores comentários a respeito, a menos que haja algum esclarecimento relevante a ser feito. Em outros casos, a adoção de bitcoins coloridas viria perfeitamente ao encontro da dinâmica interna típica do sistema de moedas complementares analisado, em outros ainda as bitcoins coloridas realizariam efeitos contrários àqueles tipicamente identificados nesses sistemas, o que poderia trazer resultados desejáveis ou indesejáveis. Tais particularidades serão discutidas a seguir. Durante a escrita iremos referenciar as "características gerais" da Tabela 3 por seu número de ordem, chamando-as simplesmente de "características" ou "aspectos" (por exemplo, característica 7: "pode ser cobrada uma taxa no ato do cadastro do participante").

Primeiramente, vejamos os reflexos positivos (ou majoritariamente positivos) em um cenário hipotético de adoção das *colored bitcoins* em qualquer das três categorias de sistemas de moedas complementares identificadas. O suporte a moedas virtuais ou eletrônicas (característica 3) pode estar presente em todos os três sistemas identificados. Isso significa que a adoção de bitcoins coloridas poderia reduzir os custos das transações eletrônicas, uma vez que o Bitcoin é definitivamente superior neste aspecto quando comparado ao dinheiro eletrônico convencional (cartões de crédito). Isso pode ser demonstrado pela ordem de grandeza das taxas cobradas para se realizar transações no Bitcoin. Como vimos anteriormente, em um cenário de crise, o valor das taxas do Bitcoin subiu para 7 centavos de dólar americano por transação (aproximadamente 25 centavos de real), enquanto as taxas básicas das operadoras de cartões de crédito facilmente passam dos 10 centavos de dólar, sem contar que há o recolhimento de taxas percentuais sobre o valor da transação, o que não ocorre no Bitcoin (DWYER, 2015). A possibilidade se de manter registro de todas as transações (característica 5) é uma outra vantagem. Tipicamente, apenas os Sistemas de Trocas Assíncronas mantém registro de todas as transações, isso dificulta a análise do comportamento dos participantes de

uma rede de trocas de uma moeda complementar em termos quantitativos, dada a ausência de registro das transações (FRAňKOVÁ, FOUSEK, *et al.*, 2014). Portanto, neste aspecto a adoção de colored bitcoins abriria a possibilidade de se realizarem análises quantitativas visando a melhoria da dinâmica interna das comunidades organizadas em torno de uma moeda complementar. Um outro aspecto interessante, é a possibilidade de realizar votações (característica 10) para concessão de empréstimos por meio das colored bitcoins. Para isso, bastaria estabelecer a regra de que um determinado montante de bitcoins só poderia ser transferido a um indivíduo caso a transação fosse assinada por todos, ou pela maioria dos votantes. Essa funcionalidade, entretanto, dependeria do conhecimento da linguagem de *scripting* do Bitcoin e da implementação por meio de uma *API*, como vimos anteriormente. Da mesma forma, um modelo de desvalorização (oxidação) da moeda em função do tempo (característica 12) é possível de ser implementado usando *colored bitcoins*. Entretanto, como no caso da votação, não existe um produto pronto (um *software* distribuído pela comunidade Bitcoin) para essa finalidade. Quanto à característica 13, em teoria, o volume de transações realizadas na rede Bitcoin é ilimitado, embora já vimos que há casos em que o limite da capacidade de processamento é atingido, o que, na prática, limita temporariamente o volume de transações.

A geração das colored bitcoins, enquanto meios de se registrar metadados, permitem que sejam guardadas qualquer informação, até mesmo uma frase como "aparei a grama na casa do Marcos hoje". Uma outra forma de utilizar esses metadados seria para definir a moeda complementar, algo como "essas *bitcoins* são equivalentes a 1 Palma". Assim, estar-se-ia criando uma moeda complementar a partir de uma *bitcoin* comum. Portanto, a escolha de gerar as *colored bitcoins* no ato da realização de uma transação (característica 14), como tipicamente ocorre nos Sistemas de Trocas Assíncronas, ou a escolha de gerar um certo montante e transferi-lo a um indivíduo (como tipicamente ocorre nos Sistemas Hours) fica a critério do modo de operação do sistema original. Entretanto, o Bitcoin definitivamente pode ser aceito pelo comércio local (característica 15), ou seja, pelo comércio externo à rede utilizadora da moeda complementar e, de fato, há vários estabelecimentos comerciais ao redor do mundo que aceitam *bitcoins*. Como uma *colored bitcoin* continua sendo uma *bitcoin*, esse aspecto não mudaria. Entretanto, o comércio local que desejasse receber as bitcoins coloridas teria que fazer uso dos mesmos aplicativos adotados pela comunidade criadora da moeda complementar, caso contrário, caso o comerciante utilize o cliente Bitcoin comum, incapaz de identificar as moedas coloridas, seu

valor enquanto *colored bitcoin* seria perdido e isso representaria uma evasão de moeda para fora do sistema original. A seguir, veremos os aspectos mais controversos e negativos da adoção de *colored bitcoins* como um sistema de moeda complementar.

A primeira consequência de se adotar bitcoins coloridas como moeda complementar seria o impacto na escolha da unidade monetária da moeda complementar (característica 1). Isso, aliado ao fato de que o Bitcoin é, para todos os efeitos, uma moeda plenamente conversível (característica 4), podendo ser comprada e vendida a partir de outras moedas oficiais, como o Dólar ou o Real, resultaria na existência de uma unidade monetária paralela àquela definida pela comunidade gestora da moeda complementar. Por exemplo, a unidade monetária no Ithaca HOURS é o valor médio da hora de trabalho (10 USD), logo, 1 HOUR vale, na prática, 10 dólares americanos. Como já vimos anteriormente, em um cenário de adoção das bitcoins coloridas como meio circulante, 1 HOUR seria, de certo modo, equivalente a aproximadamente 10.000 *satoshis*, sob a forma de *colored bitcoins*. Ora, isso faz com que 1 HOUR passe a valer apenas alguns centavos de dólar, caso o portador deste crédito de aproximadamente 10.000 *satoshis* deseje converter seu saldo em dólares americanos. Isso gera uma grande contradição que pode ser extremamente indesejável para a comunidade. Além disso, o fato de o Bitcoin ser uma moeda conversível, daria margem ao envio de *colored bitcoins* para fora do círculo de atuação da moeda complementar. Embora no caso do Ithaca HOURS o valor de conversão seja totalmente desfavorável, o que desencorajaria tal prática, nada impede que haja uma fuga de moedas em um sistema onde o valor da moeda seja meramente simbólico, sem paralelo com moedas oficiais, como ocorre nos Sistemas de Trocas Assíncronas. Portanto, a chance de que isso ocorra deve ser levada em consideração ao se cogitar a adoção de *colored bitcoins* como moeda complementar.

A impossibilidade de se emitir papel-moeda em bitcoins coloridas (característica 2) é um outro problema já explorado na seção 5.1. Entretanto, o Bitcoin, sendo uma moeda virtual descentralizada, não impõe barreiras à sua receptação (características 6 e 8). Portanto, seria possível que uma pessoa externa a uma comunidade forjasse *colored bitcoins* (emitisse *colored bitcoins* no padrão de representação da informação definido por uma comunidade alvo), as quais passariam a ser percebidas como moedas complementares daquela comunidade alvo para todos os efeitos. O efeito prático disso é que a comunidade perderia o controle da emissão e circulação de sua moeda. Logo, seria necessário implementar mecanismos de proteção à geração de moedas coloridas, de modo que somente a comunidade detivesse o conhecimento necessário, ou o código necessário, para criar uma moeda colorida sua. Entretanto, a solução para esse

problema não seria trivial, possivelmente exigindo o uso de técnicas criptográficas, o que só aumentaria a complexidade de se implementar um *software* capaz de emitir e controlar as trocas ocorridas em bitcoins coloridas. Da mesma forma, caso não exista esse mecanismo de controle da emissão de bitcoins coloridas para representar uma moeda complementar específica, não há como cobrar taxas no ato do cadastro dos participantes (característica 7), uma vez que os participantes poderiam realizar um autocadastro a partir do conhecimento de como criar uma moeda colorida que pudesse ser identificada (reconhecida pelo *software*) como a moeda complementar em questão. Um outro problema, seria a dificuldade de se cobrar taxas no ato de conversão da moeda complementar em seu lastro (característica 11) nos sistemas em que isso é permitido (tipicamente nos Sistemas de Moedas Conversíveis), pois o participante poderia optar por converter suas bitcoins coloridas em dólares, ao invés de seguir as regras da moeda complementar. Por fim, nos Sistemas de Moedas Conversíveis, dificilmente sua moeda complementar poderia ser emitida por um banco comercial (característica 16), haja vista a inexistência de validade jurídica do Bitcoin como moeda.

Comparando a compatibilidade dos 16 aspectos identificados para os três sistemas quando confrontados individualmente com a adoção de bitcoins coloridas, temos os seguinte resultado: nos Sistemas de Trocas Assíncronas, as *colored bitcoins* manteriam compatibilidade com 12 dos 16 aspectos do sistema original (75%) (aspectos 2, 3, 5, 7, 9, 10, 11 ao 16), com a vantagem de poder eliminar parcialmente o trabalho da coordenação central (aspecto 5), uma vez que não seria necessário fazer o registro de cada transação, pois esta já é uma característica intrínseca do Bitcoin. Entretanto, a coordenação central ainda seria responsável por divulgar as ofertas e demandas (aspecto 9) a fim de tornar as possibilidades de trocas conhecidas dentro da comunidade. Nos Sistemas Hours a compatibilidade também seria de 12/16 (75%) (aspectos 3, 5, 7 ao 16), mantendo três dos mesmos problemas notáveis do sistema anterior (aspectos 1, 4 e 6). A ausência de suporte a papel-moeda (aspecto 2) é um problema nesses sistemas, enquanto o recebimento de moeda por pessoas externas à comunidade é um problema nos Sistemas de Trocas Assíncronas (aspecto 8). Já nos Sistemas de Moedas Conversíveis, a compatibilidade sobe um pouquinho mais, atingindo 13/16 (81,25%). Os aspectos alvo de incompatibilidade são os itens 1, 2 e 16 da Tabela 3. O item 1 é o único problema que seria comum a todos os sistemas identificados no cenário de adoção das *colored bitcoins*, embora provavelmente não seja o mais grave, se consideradas as necessidades específicas de cada moeda complementar e a vastidão de experiências (formas de implementação) de tais moedas (RIGO, 2014). Cabe notar que cada

aspecto responde individualmente por 6.25%, dado o pequeno volume de aspectos alvos de análise (16 no total). Portanto, embora os Sistemas de Moedas Conversíveis apresentem um volume maior de compatibilidade, essa análise é qualitativa, não quantitativa.

Tabela 3 – Comparação dos Sistemas de Moedas Complementares Identificados Previamente com o Cenário de Adoção das Bitcoins Coloridas

No.	Características Gerais	Sistemas de Trocas Assíncronas	Sistemas Hours	Sistemas de Moedas Conversíveis	Bitcoins Coloridas
1	A unidade monetária é definida pela comunidade	Sim	Sim	Sim	Não
2	Há emissão de papel-moeda	Não	Sim	Sim	Não, tipicamente
3	Há uso de moeda virtual ou eletrônica	Sim (apenas para registro da transação em sistema)	Sim (a critério da comunidade)	Sim (a critério da comunidade)	Sim
4	Moeda pode ser convertida em seu lastro (moeda de curso legal ou moeda equivalente)	Não	Não	Sim	Sim
5	É necessário guardar registro de todas as transações realizadas	Sim	Não	Não	Sim, porém é intrínseco
6	É requerido cadastro prévio para participar do sistema	Sim	Tipicamente Sim	Tipicamente não	Não
7	Pode ser cobrada uma taxa no ato do cadastro do participante	Sim	Sim	Não	Sim, porém é vulnerável a evasão
8	Pessoas não cadastradas podem receber pagamentos (ou adquirir moeda)	Não	Sim	Sim	Sim

9	Ofertas e demandas são cadastradas e publicadas periodicamente	Sim	Não	Não	A critério do sistema original
10	Há votação para deliberar sobre a concessão de empréstimos	Não se aplica	Sim	Não se aplica	Sim, a depender de implementação
11	Pode haver recolhimento de taxas (ou percentuais) no ato de conversão da moeda	Não	Sim	Sim	Sim, porém sujeito a evasão
12	Pode ser aplicado algum método de desvalorização da moeda em função do tempo	Sim	Sim	Sim	Sim, a depender de implementação
13	Volume de transações é ilimitado	Depende da capacidade de se manter registro	Sim	Sim	Sim, porém sujeito a incidentes limitadores
14	Geração da moeda ocorre somente no ato de realização de uma transação entre os atores	Sim	Não	Sim (ainda que num ato de aquisição da moeda via câmbio)	A critério do sistema original
15	Possibilita a criação relações de troca com a rede de comércio formal	Não	Sim	Sim	Sim
16	Moeda complementar pode ser emitida por bancos comerciais	Não	Não	Sim	Não

(COLLOM, 2005), (BLANC, 2011), (FREIRE, 2011), (COLLOM, 2012), (VOLKMANN, 2012), (DITTMER, 2013), (RIGO, 2014)

Cabe notar que o fato de os Sistemas de Moedas Conversíveis serem aqueles que apresentaram maior compatibilidade (em quantidade de itens) com as *colored bitcoins* pode ser atribuído à maior semelhança de tais sistemas com as moedas oficiais. Como o Bitcoin é uma tecnologia candidata a ser uma moeda como outra qualquer (como uma moeda oficial), é natural que o Bitcoin apresente maior compatibilidade com sistemas de moedas complementares que permitam a livre participação, livre conversão da moeda e até mesmo a emissão de tais moedas por bancos comerciais. Portanto, podemos inferir que quanto menos regras internas restritivas

um sistema de moedas complementares possuir, maiores as chances de sucesso em um cenário de adoção do Bitcoin. Caso o Bitcoin fosse juridicamente considerado moeda, provavelmente bancos comerciais poderiam emitir moedas complementares com base em Bitcoin (característica 16), e caso a unidade monetária definida em um Sistema de Moedas Conversíveis seja a mesma unidade monetária típica do Bitcoin (dólares americanos) ou uma moeda de câmbio atrelado ao dólar americano, como o Real, possivelmente os impactos de não se atender à característica 1 seriam bastante reduzidos. Restaria apenas a incompatibilidade do papel-moeda (característica 2), o qual seria um problema de difícil solução, dada a característica criptográfica do Bitcoin.

Por fim, discutiremos as vulnerabilidades identificadas nos três sistemas de moedas complementares e como o uso das *colored bitcoins* resolveria ou agravaria o problema. A vulnerabilidade 1 não sofreria qualquer alteração com a adoção de bitcoins coloridas, pois as regras de concessão de crédito seriam ainda um arbítrio dos gestores de sistemas de moedas complementares, ou da comunidade. A vulnerabilidade 2, a qual afeta os Sistemas de Trocas Assíncronas pode ser resolvida pelo uso de colored bitcoins, fato já discutido anteriormente. A vulnerabilidade 3 seria potencialmente agravada ao se adotar Bitcoins como moeda complementar, pois um surto de valorização das bitcoins poderia levar a uma fuga de moedas dos sistemas de moedas complementares. A vulnerabilidade 4, que também só afeta os Sistemas de Trocas Assíncronas, seria parcialmente resolvida pela adoção de *colored bitcoins*, fato também já explicado anteriormente. A vulnerabilidade 5, também particular dos Sistemas de Trocas Assíncronas poderia ser potencialmente resolvida pela adoção de bitcoins coloridas, já que é possível eliminar a tarefa de controlar e registrar as transações tipicamente realizado pela coordenação central e, como isso, as partes de cada transação ficariam livres para discutir o valor da mão-de-obra sem o arbítrio da coordenação central. Por fim, a vulnerabilidade 6 também ficaria a critério do sistema original. Cabe notar, novamente, que estabelecer bloqueios

ou limites à aceitação de bitcoins coloridas, não seria uma tarefa trivial, dependendo de condições específicas por meio da linguagem Script do Bitcoin e das *APIs* das *colored bitcoins*.

Tabela 4 – Comparação das Vulnerabilidades Identificadas Previamente nos Sistemas de Moedas Complementares com o Cenário de Adoção das Bitcoins Coloridas

No.	Vulnerabilidades	Sistemas de Trocas Assíncronas	Sistemas Hours	Sistemas de Moedas Conversíveis	Bitcoins Coloridas
1	Vulnerável a acumulação excessiva de débitos ou de créditos	Sim (débitos)	Sim (créditos)	Não	A critério das regras do sistema original
2	Volume de transparência contábil requerido cresce na mesma proporção do número de participantes	Sim	Não	Não	Não
3	Vulnerável a especulação desestabilizadora e inflação	Não	Sim	Sim	Sim
4	Requer uma administração central para registrar todas as transações, ofertas e demandas	Sim	Não	Não	Não
5	Ocorrem conflitos de definição de preços em função da qualidade do trabalho individual	Sim	Não	Não	Não
6	Deve-se impor limites à aceitação da moeda a fim de evitar acúmulo de crédito (ou limitar a contração de débito) por indivíduo	Sim	Sim	Não	A critério das regras do sistema original

(COLLOM, 2005), (BLANC, 2011), (FREIRE, 2011), (COLLOM, 2012), (VOLKMANN, 2012), (DITTMER, 2013), (RIGO, 2014)

6 CONSIDERAÇÕES FINAIS

O estudo aprofundado e comparado da literatura a respeito das moedas complementares foi um instrumento essencial para a identificação das principais características das moedas ditas locais, sociais, comunitárias ou complementares, as quais passamos a chamar apenas de "moedas complementares", como termo capaz de agrupar os demais especialmente a partir de Collom (2011), Freire (2011) e Rigo (2014). Para a criação de um sistema de classificação, estabelecendo classes capazes de agrupar as diferentes experiências relatadas na literatura, foi necessário um aprofundamento teórico, por meio de Blanc (2011), e foi útil a classificação proposta por Rigo (2014), bem como alguns aspectos identificados em Freire (2011). Para que fosse possível descrever o funcionamento do Bitcoin, identificando suas motivações, as circunstancias de seu surgimento, a teoria que embasa o protocolo e os componentes chave que o sustentam, foi necessária a consulta a diversas fontes informais, notavelmente conversas em fóruns na *Internet*, a *Bitcoin Wiki* (enciclopédia oficial do Bitcoin) e os trabalhos de Nielsen (2013) e de Shirriff (2016), dada a ausência de estudos científicos completos e didáticos o suficiente para substituir a consulta a essas fontes informais. A mesma abordagem foi necessária para explicar como as *colored bitcoins* são implementadas em cima da estrutura do protocolo Bitcoin. Por fim, para identificar as potencialidades e as fraquezas do uso das *colored bitcoins* como moeda, analisando seu nível de compatibilidade com cada classe definida previamente, foi necessário um exercício de análise comparada de suas características, à luz de todo o conhecimento obtido durante o desenvolvimento deste trabalho.

As hipóteses iniciais, que motivaram os estudos realizados neste trabalho puderam ser parcialmente validadas. A capacidade de eliminar a necessidade de se ter uma gerência responsável pela coordenação da mecânica de funcionamento das moedas complementares pode ocorrer parcialmente nos Sistemas de Trocas Assíncronas, porém é improvável que deva ocorrer, ainda que parcialmente nos outros dois sistemas (Sistemas Hours e Sistemas de Moedas Conversíveis), pois as *colored bitcoins* não poderiam eliminar todas as decisões gerenciais, dado que a própria implementação de um sistema (*software*) que irá criar e gerenciar as *colored bitcoins* iria requerer a existência de uma coordenação responsável por tomar esta decisão. A substituição da emissão de papel-moeda mostrou-se possível apenas em casos muito particulares, em que se possa manter um baixo custo de adoção do Bitcoin como meio circulante e se possa assumir os riscos de ter transações não confirmadas durante um potencial evento de interrupção do processamento de transações na rede Bitcoin. Por fim, a substituição do uso de cartões de crédito, eliminando, assim, as taxas cobradas por suas operadoras e a necessidade de

se alugar máquinas de processamento de pagamento se mostrou viável, já que o Bitcoin de fato opera com taxas muito mais baixas. Entretanto, o Bitcoin também trabalha com cobrança de taxas as quais tendem a aumentar conforme se reduz o valor da recompensa por bloco minerado.

A análise comparada da literatura a respeito das moedas comunitárias, identificando os casos pioneiros e os casos mais citados pelos autores, foi essencial para que se atingisse o objetivo de definir classes de moedas comunitárias com base em suas características técnicas principais. Tal classificação tornou possível comparar os modelos de moedas comunitárias existentes entre si e, principalmente, com as bitcoins coloridas, as quais supostamente seriam uma moeda complementar virtual genérica, passível de ser utilizada como base tecnológica para fins de se criar qualquer outra moeda complementar. O estudo aprofundado do protocolo Bitcoin, nos seus aspectos técnicos, jurídicos, econômicos e sociais, bem como a análise precisa de como as bitcoins coloridas são de fato implementadas em cima da infraestrutura deste protocolo, permitiu-nos analisar de forma completa as implicações que a adoção de tal tecnologia traria para uma comunidade que já possua ou pretenda criar uma moeda complementar. Vimos que, dado o alto grau de comprometimento (*trade-offs*), não seria recomendável adotar o Bitcoin em larga escala, mas apenas em pequenos sistemas onde fosse possível observar de perto os impactos de tal tecnologia.

A partir da classificação proposta por este trabalho é possível conhecer de antemão diversos aspectos relevantes das moedas complementares existentes. Isso permitirá, por exemplo, analisar um caso particular de uma moeda complementar que se deseje criar já durante a sua idealização, avaliando o seu projeto sob a ótica do que é relevante em moedas comunitárias de sucesso. Outra contribuição relevante deste trabalho é permitir que se avalie a viabilidade de se adotar as *colored* bitcoins como tecnologia exclusiva ou complementar na criação de uma moeda complementar. Por exemplo, no cenário hipotético de criação de uma moeda complementar no Instituto de Computação da UFF, a qual poderia, dentre outros casos de uso, ser usada para representar as relações de troca de horas de atividades complementares por créditos curriculares, recairia sem dúvida na categoria de um Sistema de Trocas Assíncronas, tendo o tempo como sua unidade básica de valor. Os impactos da adoção do Bitcoin em tal sistema seriam, portanto, os mesmos identificados e discutidos na seção anterior, notavelmente a dificuldade de se impor barreiras à participação de pessoas externas à comunidade acadêmica e a dificuldade de impedir a forja de moedas coloridas, as quais poderiam ter origem não acadêmica (até mesmo sendo compradas a partir da *Internet*) e seriam, ainda assim, aceitas pelo

sistema que processasse sua conversão em créditos de atividades complementares como moeda legítima.

Uma limitação relevante deste trabalho reside no fato de que a classificação por nós proposta não pode ser tomada em termos absolutos, ou seja, ela foi concebida com base em aspectos selecionados a partir da literatura. Portanto, tal classificação não pode ser adotada como referencial absoluto para se entender as implicações do uso das *colored bitcoins* como moeda complementar, mas pode apenas ser usada nos casos em que a moeda complementar em questão possa ser facilmente descrita nos termos da classificação proposta por este trabalho. Porém, a principal limitação deste trabalho reside no escopo da literatura consultada, o qual ficou restrito a publicações em português e em inglês, e tal limitação poderia restringir ainda mais a abrangência da classificação proposta. Tanto as moedas comunitárias quanto o Bitcoin são assuntos pouco explorados pela literatura em geral, fato apontado por diversos autores em suas publicações. Portanto, não se pode considerar que as fontes consultadas sejam capazes de cobrir a maioria dos modelos de moedas que tenham sido ou que venham a ser criados em algum momento, mas apenas se pode considerar que elas abrangem os modelos mais notáveis. Uma análise da literatura sobre moedas comunitárias realizada pelo *International Journal of Community Currency Research* em 2011 revelou que a maioria das contribuições científicas sobre este assunto eram realizadas em língua inglesa, respondendo por 37% das publicações. Entretanto, as contribuições publicadas em japonês, francês e espanhol respondiam respectivamente por 18%, 9% e 6%. Esses são percentuais bastante significativos, especialmente quando se leva em conta que, somados, respondem por 33% das publicações, um volume quase tão grande quanto o de todas as publicações em língua inglesa. Além disso, a grandeza de tais números se destaca ainda mais quando se verifica que as contribuições em língua portuguesa respondiam por apenas 1% das publicações na base de dados utilizada como referência para aquela pesquisa (SCHROEDER, MIYAZAKI e FARE, 2011). Isso torna a restrição das fontes de consulta em função da língua uma limitação bastante relevante.

Uma outra limitação relevante diz respeito à quantidade de aspectos qualitativos identificados para fins de comparação entre os sistemas de moedas complementares quanto a sua compatibilidade com o Bitcoin (16 aspectos no total). Não é possível medir a expressividade dessa quantidade de aspectos identificados, pois não há referencial de comparação. Portanto, não sabemos se foram identificados poucos aspectos, ou se 16 aspectos é uma quantidade bastante representativa do conjunto de experiências analisadas. Logo, não há como considerar

o valor quantitativo do nível de compatibilidade das *colored bitcoins* com os sistemas identificados, apenas o nível de compatibilidade qualitativo de cada aspecto.

Como trabalhos futuros, seria interessante ir em busca de um refinamento para a classificação proposta por este trabalho, procurando rever os aspectos qualitativos identificados e adotados como referência para a análise comparativa. Uma outra possibilidade, seria a realização de um estudo de caso em que se realizasse uma análise prévia de um cenário específico em que se deseje criar uma moeda complementar com base em *colored bitcoins*, verificando se as conclusões das análises apresentadas neste trabalho se mostrariam verdadeiras no caso aplicado.

REFERÊNCIAS

AHN, L. V. et al. Human-Based Character Recognition via Web Security Measures. **Science Magazine**, 12 Setembro 2008.

ALMEL; NAYUKI. Explanation of what an OP_RETURN transaction looks like. **Bitcoin Stack Exchange**, 2015. Disponivel em: <http://bitcoin.stackexchange.com/questions/29554/explanation-of-what-an-op-return-transaction-looks-like>. Acesso em: 28 Março 2016.

ANDERSEN, G. script: reduce OP_RETURN standard relay bytes to 40. **GitHub**, 2014. Disponivel em: <https://github.com/bitcoin/bitcoin/pull/3737>. Acesso em: 03 Março 2016.

AVERAGE Number of Transactions per Block. **Blockchain Info**, 2016. Disponivel em: <https://blockchain.info/charts/n-transactions-per-block>. Acesso em: 28 Março 2016.

BITCOIN Charts. **Crypto-Currency Market Capitalizations**, 2016. Disponivel em: <http://coinmarketcap.com/currencies/bitcoin/>. Acesso em: 28 Março 2016.

BITCOIN Core. **Bitcoin Wiki**, 2016. Disponivel em: <https://en.bitcoin.it/wiki/Bitcoin_Core>. Acesso em: 28 Março 2016.

BLANC, J. Classifying “CCs”: Community, complementary and local currencies’ types and generations. **International Journal of Community Currency Research**, v. 02, n. D4-10, 2011.

BLANC, J. Thirty Years of Community And Complementary Currencies: A Review Of Impacts, Potential And Challenges. **International Journal of Community Currency Research**, 2012.

BLOCK. **Bitcoin Wiki**, 02 Março 2016. Disponivel em: <https://en.bitcoin.it/wiki/Block>. Acesso em: 03 Março 2016.

BLOCK chain. **Bitcoin Wiki**, 2016. Disponivel em: <https://en.bitcoin.it/wiki/Block_chain>. Acesso em: 28 Março 2016.

BLOCK size limit controversy. **Bitcoin Wiki**, 2016. Disponivel em: <https://en.bitcoin.it/wiki/Block_size_limit_controversy>. Acesso em: 28 Março 2016.

BOTSMAN, R. The currency of the new economy is trust. **TED**, 2012. Disponivel em: <Rachel Botsman: The currency of the new economy is trust>. Acesso em: 03 Março 2012.

BOTSMAN, R. Defining The Sharing Economy: What Is Collaborative Consumption—And What Isn't? **Co.Exist**, 05 Maio 2015. Disponivel em:

<http://www.fastcoexist.com/3046119/defining-the-sharing-economy-what-is-collaborative-consumption-and-what-isnt>.

BUTERIN, V. Bitcoin Magazine. **Bitcoin in Israel:** Interview with Meni Rosenfeld and Ron Gross, Part I, 2013. Disponivel em: <https://bitcoinmagazine.com/articles/bitcoin-in-israel-interview-with-meni-rosenfeld-and-ron-gross-part-i-1382036609>. Acesso em: 03 Março 2016.

CAMINHA, U.; FIGUEIREDO, M. Atividade financeira e moeda: análise da experiência do Conjunto Palmeiras em Fortaleza-CE. **Revista Direito GV**, Janeiro a Julho 2011.

COLLOM, E. Community currency in the United States: the social environments in which it emerges and survives. **Environment and Planning A**, 2005. ISSN DOI:10.1068/a37172.

COLLOM, E. Motivations and Differential Participation in a Community Currency System: The Dynamics Within a Local Social Movement Organization. **Sociological Forum**, Março 2011.

COLLOM, E. Key Indicators of Time Bank Participation: Using Transaction Data for Evaluation. **International Journal of Community Currency Research**, v. 16, 2012.

COLORED Coins. **bitcoinwiki**, 03 Março 2016. Disponivel em: <https://en.bitcoin.it/wiki/Colored_Coins>.

CYPHERPUNKS Mailing List. **Cypherpunks**, 2016. Disponivel em: <https://www.cypherpunks.to/list/>. Acesso em: 28 Março 2016.

DIFFICULTY. **Bitcoin Wiki**, 2016. Disponivel em: <https://en.bitcoin.it/wiki/Difficulty>. Acesso em: 28 Março 2016.

DITTMER, K. Local currencies for purposive degrowth? A quality check of some proposals for changing money-as-usual. **Journal of Cleaner Production**, 2013.

DWYER, B. Credit Card Processing Fees & Rates. **Card Fellow**, 2015. Disponivel em: <https://www.cardfellow.com/credit-card-processing-fees/#GettingLowestRates>. Acesso em: 28 Março 2016.

FARIA, L. A. S. D. Softwares Livres, Economia Solidária e o Fortalecimento de Práticas Democráticas : Três Casos Brasileiros. **COPPE/UFRJ**, 2010.

FARIA, L. A. S. D. Bitcoin: materialidades, liberdades e interações de uma moeda-rede, 2015.

FRAňKOVÁ, E. et al. Transaction network analysis for studying Local Exchange Trading Systems (LETS): Research potentials and limitations. **Ecological Economics**, v. 107, 2014. ISSN http://dx.doi.org/10.1016/j.ecolecon.2014.09.009.

FREIRE, M. V. Moedas Sociais: Contributo Em Prol De Um Marco Legal E Regulatório Para As Moedas Sociais Circulantes Locais No Brasil. **Universidade de Brasília (UNB)**, 2011.

FULL Validation. **Bitcoin.org**, 2016. Disponivel em: <https://bitcoin.org/en/bitcoin-core/features/validation>. Acesso em: 28 Março 2016.

GARAY, J.; KIAYIAS, A.; LEONARDOS, N. The Bitcoin Backbone Protocol: Analysis and Applications. In: _____ **Advances in Cryptology - EUROCRYPT 2015**. [S.l.]: Springer, 2015.

GREENBERG, A. New Clues Suggest Craig Wright, Suspected Bitcoin Creator, May Be a Hoaxer. **Wired**, 2015. Disponivel em: <http://www.wired.com/2015/12/new-clues-suggest-satoshi-suspect-craig-wright-may-be-a-hoaxer/>. Acesso em: 28 Março 2016.

GROVE, A.; BERG, G. A. **Social Business:** Theory, Practice, and Critical Perspectives. California: Springer, 2014.

HILL, K. Satoshi Nakamoto's Email Provider Sheds Little Light On The Hacking And Deletion Of Bitcoin Creator's Account. **Forbes**, 2014. Disponivel em: <http://www.forbes.com/sites/kashmirhill/2014/09/16/satoshi-nakamoto-email-hack/#3c779c715fec>. Acesso em: 30 Março 2016.

KIM, T. The Predecessors of Bitcoin and Their Implications for the Prospect of Virtual Currencies. **PLoS ONE**, Abril 2015.

LEARN. **Colu**, 2016. Disponivel em: <https://www.colu.co/learn>. Acesso em: 28 Março 2016.

LEE, J. et al. Bitcoin Basics: a Primer on Virtual Currencies. **Business Law International**, Janeiro 2015.

NAKAMOTO, S. Bitcoin: A Peer-to-Peer Electronic Cash System, 2009.

NAKAMOTO, S. Forum: Bitcoin open source implementation of P2P currency. **P2P Foundation**, 11 Fevereiro 2009. Disponivel em: <http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source>.

NIELSEN, M. Open science now! **TED Talk**, 2011. Disponivel em: <https://www.ted.com/talks/michael_nielsen_open_science_now>. Acesso em: 28 Março 2016.

NIELSEN, M. How the Bitcoin protocol actually works. **Data Driven Intelligence**, 2013. Disponivel em: <http://www.michaelnielsen.org/ddi/howthebitcoinprotocolactuallyworks/>. Acesso em: 28 Março 2016.

ONGARATTO, N. Bitcoins devem ser declaradas no IR de 2016. **Investimentos e Notícias**, 2016. Disponivel em: <http://www.investimentosenoticias.com.br/noticias/imposto-de-renda-2016/bitcoins-devem-ser-declaradas-no-ir-de-2016>. Acesso em: 03 Março 2016.

PAPER Wallet. **Bitcoin Wiki**, 2016. Disponivel em: <https://en.bitcoin.it/wiki/Paper_wallet>. Acesso em: 03 Março 2016.

PROOF of work. **Bitcoin Wiki**, 2016. Disponivel em: <https://en.bitcoin.it/wiki/Proof_of_work>. Acesso em: 28 Março 2016.

PROTOCOL Documentation. **Bitcoin Wiki**, 02 Março 2016. Disponivel em: <https://en.bitcoin.it/wiki/Protocol_documentation>.

RECOMMENDED Bitcoin Network Transaction Fees. **Bitcoin Exchange Rate**, 2016. Disponivel em: <http://bitcoinexchangerate.org/fees>. Acesso em: 28 Março 2016.

REDMAN, J. An Introduction to the Cypherpunk Tale. **Bitcoin News**, 2015. Disponivel em: <https://news.bitcoin.com/introduction-cypherpunk-tale/>. Acesso em: 28 Março 2016.

RIGO, A. S. Moedas Sociais e Bancos Comunitários no Brasil: Aplicações e Implicações, Teóricas e Práticas. **Universidade Federal da Bahia**, 2014.

ROSENFELD, M. Overview of Colored Coins, 2012.

SATOSHI Nakamoto's Page. **P2P Foundation**, 2016. Disponivel em: <http://p2pfoundation.ning.com/profile/SatoshiNakamoto>. Acesso em: 28 Março 2016.

SATOSHIN@GMX.COM is compromised. **Bitcoin Forum**, 2014. Disponivel em: <https://bitcointalk.org/index.php?topic=775174.msg8734884#msg8734884>. Acesso em: 28 Março 2016.

SCHROEDER, R. F. H.; MIYAZAKI, Y.; FARE, M. Community Currency Research: An Analysis Of The Literature. **International Journal of Community Currency Research**, 2011.

SCRIPT. **Bitcoin Wiki**, 2016. Disponivel em: <https://en.bitcoin.it/wiki/Script>. Acesso em: 28 Março 2016.

SHIRRIFF, K. Bitcoins the hard way: Using the raw Bitcoin protocol. **Ken Shirriff's blog**, 02 Março 2016. Disponivel em: <http://www.righto.com/2014/02/bitcoins-hard-way-using-raw-bitcoin.html>.

SILVA, C. E. G. Gestão, legislação e fontes de recursos no terceiro setor brasileiro: uma perspectiva histórica. **Revista de Administração Pública FGV**, Novembro e Dezembro 2010.

SIMONITE, T. The Looming Problem That Could Kill Bitcoin. **MIT Technology Review**, 2015. Disponivel em: <https://www.technologyreview.com/s/540921/the-looming-problem-that-could-kill-bitcoin/>. Acesso em: 28 Março 2016.

SIMONITE, T. Bitcoin hit a capacity limit that could hamper dreams of it becoming widely used. **MIT Technology Review**, 2016. Disponivel em: <https://www.technologyreview.com/s/600941/bitcoin-transactions-get-stranded-as-cryptocurrency-maxes-out/#/set/id/600935/>. Acesso em: 28 Março 2016.

SIMONITE, T. Technical Roadblock Might Shatter Bitcoin Dreams. **MIT Technology Review**, 2016. Disponivel em: <https://www.technologyreview.com/s/600781/technical-roadblock-might-shatter-bitcoin-dreams/>. Acesso em: 28 Março 2016.

TRIPUNITARA, M.; MESSERGES, T. Resolving the Micropayment Problem. **IEEE Computer Society**, Fevereiro 2007.

VANDERVORT, D.; GAUCAS, D.; JACQUES, R. S. Issues in Designing a Bitcoin-like Community Currency. In: _____ **Financial Cryptography and Data Security**. [S.l.]: Springer, 2015.

VIILUP, K. Profitability From Mining Bitcoins: Should You Still Enter The Bitcoin Mining Competition? Long-Term Simulation Analysis Of The Profitability For A Single Miner. **University of Tartu**, Estonia, 2015.

VOLKMANN, K. Solidarity Economy Between A Focus On The Local And A Global View. **International Journal of Community Currency Research**, 2012.

WALLET. **Bitcoin Wiki**, 02 Março 2016. Disponivel em: <https://en.bitcoin.it/wiki/Wallet>. Acesso em: 03 Março 2016.

YUNUS, M. **Building social business:** the new kind of capitalism that serves humanity's most pressing needs. New York: Public Affairs, 2010.

ZAMPIERI, G. C. Natureza jurídica e tributação da bitcoin. **Jusbrasil**, 2015. Disponivel em: <http://gczampieri.jusbrasil.com.br/artigos/118688250/natureza-juridica-e-tributacao-da-bitcoin>. Acesso em: 28 Março 2016.

GLOSSÁRIO

Alvo É um número de 256 bits, utilizado como componente do processo de mineração de bitcoins. A função do alvo é estabelecer uma meta para o valor do *hash* do cabeçalho de um bloco, de modo que ao validar um bloco o *hash* gerado deve estar abaixo do alvo para que seja aceito pela rede. Quanto menor o alvo (maior quantidade de zeros à esquerda), mais difícil é encontrar a solução.

B2C Do inglês *Business to Consumer* (Empresa-Consumidor). Esse termo designa um dos modelos de negócios característicos do comércio eletrônico (*e-commerce*), ou de prestação de serviços em que em uma ponta se tem uma entidade pessoa jurídica, uma empresa, e na outra ponta se tem os consumidores.

Bitcoin Com b maiúsculo, é usado neste trabalho para designar o sistema, ou seja, o protocolo Bitcoin e todas as existentes implementações de clientes Bitcoin existentes que tornam esse protocolo operacional. Esse protocolo é especificado pelo comportamento do programa cliente de referência, criado por Satoshi Nakamoto em 2009.

bitcoin Com b minúsculo, é usado neste trabalho para designar a moeda bitcoin, ou BTC, a qual pode ser obtida como recompensa ou comprada via pagamento em outras moedas, comumente o Dólar Americano (USD).

Bitcoin Core Vide “cliente Bitcoin”

Bitcoin Wiki Enciclopédia oficial do Bitcoin, acessível a partir do site *en.bitcoin.it*

Bitcoins coloridas Vide *colored bitcoins*.

Block chain Ou *blockchain* é a cadeia formada pelo agrupamento sequencial de blocos de operações válidas do Bitcoion. O *block chain* é um componente essencial do protocolo Bitcoin e pode ser considerado um livro-razão público, em que todas as transações em bitcoins já realizadas podem ser consultadas. Em termos técnicos, o *block chain* pode ser considerado um *log* em função do tempo de todas as transações ocorridas na rede P2P.

Bloco É o nome dado ao arquivo contendo um cabeçalho com campos padrão e um conjunto de transações, as quais foram agrupadas em tal arquivo por um determinado nó da rede Bitcoin para fins de validação.

C2C Do inglês *Consumer to Consumer* (Consumidor-Consumidor). Esse termo designa um dos modelos de negócios característicos do comércio eletrônico (do inglês, *e-commerce*) em que não existe intermediário entre os consumidores, portanto os consumidores podem acumular as funções de vendedores ou de prestadores de serviços e realizar transações diretamente com outros consumidores.

Cliente Bitcoin É a suíte de aplicativos que implementa o protocolo Bitcoin em sua totalidade, permitindo, assim, o seu uso. A terceira versão do cliente de referência, aquele adotado pela comunidade Bitcoin, é chamada *Bitcoin Core*.

Coinbase É o nome dado ao conteúdo do campo "*input*", ou "entradas", de um bloco especial de transação que ocorre na rede Bitcoin, o qual contém o registro da geração de moedas pagas ao nó responsável pela validação de um bloco. Transações comuns sempre fazem referência à transação mãe (*parent transaction*), enquanto uma transação do tipo *coinbase* é órfã por definição, visto que ela gera moedas novas no sistema, portanto as *bitcoins* registradas em uma *coinbase* são criadas do nada, sem origem anterior.

Colored bitcoins Traduzido neste trabalho como bitcoins coloridas, são bitcoins que recebem uma camada extra de informação em alguns "campos do protocolo", permitindo, assim, que se adicionem significados a tais moedas, expandindo os casos de usos possíveis dentro da estrutura existente do Bitcoin.

Comunidade Bitcoin É a comunidade *ad hoc* formada pelas pessoas responsáveis por manter o código dos *softwares* utilizados na suíte Bitcoin (*Bitcoin Core*), pelas pessoas que tomam qualquer decisão de *design* (ou a respeito do futuro dessa suíte de aplicativos) e, também, pelas pessoas que escrevem a documentação ou material de divulgação do Bitcoin, especialmente dos *sites bitcoin.org* e *en.bitcoin.it*

Conta É um recurso que pode ser utilizado para subdividir o saldo de uma carteira Bitcoin de forma a atribuir significados a cada subconjunto. A conta nada mais é que uma *string* associada a nenhum ou mais endereços Bitcoin, representando, por exemplo, uma fonte de recursos específica ou uma destinação específica de pagamentos realizados pelo usuário.

Dificuldade Medida do quão difícil é encontrar a solução para um bloco de operações (*hash*) abaixo de um determinado alvo. A dificuldade é ajustada a cada 2016 blocos validados, com vistas a manter a média do tempo de surgimento de um bloco validado na rede em torno de 10 minutos. A essa taxa de validação, a rede deveria receber 2016 blocos validados a cada duas semanas.

Duplo SHA-256 Técnica criptográfica que consiste em utilizar o algoritmo SHA-256 duas vezes seguidas.

Endereço É um identificador alfanumérico, sensível a maiúsculas e minúsculas, contendo de 26 a 35 caracteres, que representa um destino para onde pagamentos em *bitcoins* podem ser enviados apenas uma vez, pois esse identificador é de uso único por operação. Transações realizadas no protocolo Bitcoin não possuem um endereço de origem, apenas um endereço de destino, o qual é protegido pelo uso de criptografia de chave pública, de modo que apenas o detentor da chave privada pode receber as bitcoins enviadas para o endereço vinculado a uma dada chave pública. Cada endereço possui alguns caracteres com função de dígito verificador, a fim de possibilitar a identificação de erros de digitação, algo similar ao que ocorre com códigos de barra. O reuso de endereços é possível, porém deve ocorrer apenas de forma acidental, já que o reuso intencional permitiria a identificação do usuário e de suas transações, o que infringiria a proteção à segurança e à privacidade do usuário, indo contra os princípios do protocolo Bitcoin.

Genesis block Podendo ser traduzido como “bloco original”, é o primeiro bloco da *block chain*. De acordo com a *bitcoinwiki*, esse bloco é geralmente criado como parte do código original do protocolo. O genesis block do Bitcoin contém o cabeçalho da matéria de capa publicada no *The Times*

em 03 de janeiro de 2009, como prova da não existência de *bitcoins* anteriores àquela data.

Hardware wallet É uma melhor alternativa à *paper wallet* para se atingir o objetivo de proteção contra ataques de *softwares* maliciosos. A implementação consiste, basicamente, no uso de micro controladores específicos para implementar as funções de uma *wallet*, com a vantagem de não ser necessário importar as transações para a o computador posteriormente, como ocorre com a *paper wallet*.

Litecoin De forma análoga ao Bitcoin, este termo é usado para designar o conjunto de tecnologias que implementam o Litecoin.

litecoin De forma análoga ao bitcoin, este termo é usado para designar a moeda litecoin.

Mineração É o nome dado ao processo de validação de um bloco de operações realizadas na rede do Bitcoin. A conclusão do processo de validação de um bloco resulta em emissão de bitcoins para o nó que realizou a tarefa, aumentando, assim, a quantidade de bitcoins circulantes no sistema.

Mineradores Nós da rede Bitcoin (pessoas ou corporações) que realizam a tarefa de validação de transações conhecida como mineração.

Moeda complementar Neste trabalho considera-se moeda complementar qualquer moeda de origem privada que seja caracterizada por ter circulação e aceitação embasadas na adesão voluntária de um determinado grupo àquele meio de pagamento, podendo existir sob a alcunha de moeda social ou de moeda comunitária, sem vínculo obrigatório com a moeda nacional, e sem limitação de uso definida exclusivamente em função da territorialidade.

Negócios sociais no escopo deste trabalho, chamamos de negócios sociais aqueles que seguem a linha de negócios inaugurada por Muhammad Yunus, também conhecido como modelo Grameen.

P2P do inglês *peer-to-peer*, pode ser traduzido como ponto-a-ponto. Esse termo designa um modelo arquitetural para aplicações distribuídas em uma redes de computadores em que não há um ponto da rede que seja exclusivamente o servidor, em oposição aos clientes. Ao invés disso, mais de um ponto da rede pode exercer as funções de servidor e de cliente de forma concomitante ou alternada com outros servidores/clientes.

Paper wallet Traduzido como "carteira em papel", é uma forma de guardar toda a informação necessária para a geração de chaves privadas Bitcoin de um determinado usuário em um meio físico não eletrônico, notavelmente o papel. Essa solução surgiu como forma de evitar o uso da *wallet* digital, aumentando assim a proteção contra ataques realizados por aplicativos maliciosos (vírus) ou *hackers*. A impressão de uma carteira em papel envolve certos riscos e abordagens técnicas próprias para mitiga-los.

Proof-of-work Do inglês, prova do trabalho, ou prova do trabalho executado. É um sistema utilizado em criptografia para prevenir determinadas classes de ataques, como ataque de negação de serviço, em que o atacante se beneficia da inexistência de barreiras à ação rápida e iterativa do atacante. Com a prova do trabalho executado, é necessário produzir uma prova que demanda grande esforço computacional para que se possa realizar determinada ação, prevenindo, assim, a ação contínua e repetida do atacante.

Recompensa É o valor pago em *bitcoins* a um nó da rede pela validação de um bloco de operações. O valor inicial da recompensa é de 50 bitcoins. Esse valor é programado para ser reduzido pela metade a cada 210.000 blocos validados, o que aconteceria aproximadamente a cada quatro anos, já que o protocolo Bitcoin constantemente se auto regula para manter a taxa de um bloco validado a cada 10 minutos.

satoshi Nome convencional dado a unidade monetária do Bitcoin. É equivalente a 0.00000001 BTC, ou $1*10^{-8}$ bitcoins.

SHA-2 Algoritmo que descreve uma função de espalhamento (*hash*) criado pela NSA, o qual é utilizado como parte essencial do protocolo Bitcoin.

Sistemas de Moedas Complementares	Cunhamos este termo para designar o equivalente a *currency schemes*, presente na literatura inglesa. Esse termo designa uma moeda complementar enquanto um sistema, contendo uma coordenação que o administra, regras internas próprias, relacionamento com pessoas e com outros sistemas.
Terceiro setor	Embora terceiro setor não seja um nome oficial, adotamos a definição do que se entende como terceiro setor pelo Código Civil Brasileiro, que são instituições jurídicas de direito privado que exercem função de interesse público, constituídas sob a forma de fundações ou associações.
TIC	Tecnologias da Informação e Comunicação. Estão abarcados por esse conceito, dentre outros, os computadores pessoas, os telefones celulares e as redes de computadores e de telefonia.
Wallet	Também chamada *software wallet*, podendo ser traduzido como "carteira", é um arquivo contendo pares de chaves para cada um dos endereços do usuário, as contas daquele usuário, preferências e outras informações relevantes. A *wallet* exerce uma função semelhante à de um banco privado, particular, de um único usuário, onde há várias contas associadas a endereços e um saldo total referente ao conjunto das contas.