DOI: 10.5102/un.gti.v6i1.3855

O processo de negócio do sistema de transações financeiras Bitcoin*

The business process of the Bitcoin financial transaction system

José Gladistone da Rocha[1]
Carlo Kleber da Silva Rodrigues[2]

Resumo

O protocolo Bitcoin foi proposto há cerca de seis anos e sua adoção para a implementação de um sistema de transações financeiras tem se mostrado crescente em diferentes países no mundo. No entanto, há poucas obras na literatura voltadas ao esclarecimento de todas as etapas que envolvem o processo de negócio desse sistema. Nesse contexto, este artigo tem o objetivo de apresentar a modelagem desse processo de negócio bem como detalhar como ocorre o seu processo primário Gerenciar Pagamento. Para tanto, são empregadas técnicas de Engenharia de Software e de Business Process Model and Notation. Os modelos desenvolvidos permitem mapear problemas críticos do sistema, explicitando em quais etapas do processo de negócio eles incidem. Isso viabiliza principalmente a proposição mais efetiva de soluções e otimizações com vistas à maior robustez global do sistema.

Palavras-chave: Bitcoin. Engenharia de Software. Modelo. Processo de negócio. Sistema.

Abstract

The Bitcoin protocol was proposed about six years ago and its adoption for the implementation of a financial transaction system has attracted great attention all over the world. However, there are very few works in the literature aimed at clearing all stages involved in the business process of this system. Within this context, this article aims at presenting the overall modeling of this process as well as detailing how its primary process called Payment Management is carried out. To this end, techniques of Software Engineering and Business Process Model and Notation are both used. The models developed herein allow to efficiently mapping critical system issues. This mainly enables achieving more effective solutions and optimizations, providing an overall robustness to the system.

Keywords: Bitcoin. Software Engineering. Model. Business process. System.

Abreviações: Business Process Management (BPM). Business Process Model and Notation (BPMN). Engenharia de Software (ES). Metodologia de Desenvolvimento de Software (MDS). Bitcoin (BTC).

* Recebido em: 04/02/2016.
Aprovado em: 08/03/2016.

[1] Mestre em Ciências Militares pela Escola de Aperfeiçoamento de Oficiais do Exército (EsAO) (1994). Bacharel em Ciências Militares pela Academia Militar das Agulhas Negras (AMAN) (1985). Bacharel em Sistemas de Informação pelo Centro Universitário do Sul de Minas (UNIS) (2014). Pós-Graduado em Analise de Sistemas pelo Centro de Estudos de Pessoal do Exército; Pós-Graduado em Criptografia e Segurança em Redes de Computadores pela Universidade Federal Fluminense (UFF) e Pós-Graduado em Docência do Ensino Superior, pela Universidade Castelo Branco (UCB). Atua na área de Ciência da Computação, com ênfase em Desenvolvimento de Sistemas, Criptografia e Segurança em Redes de Computadores e Gestão e Governança de TI. Foi membro do Comitê Executivo de Tecnologia da Informação do Exército (2014). Leciona em Instituições de Ensino Superior de Brasília-DF. Trabalhou como Gerente e Analista de Sistemas no Centro de Desenvolvimento de Sistemas do Exército, em Brasília-DF (2006-2013). Trabalhou como Analista de Sistema do Ministério da Defesa no sistema SISCAPED (2014).

[2] Possui graduação em Engenharia Elétrica pela Universidade Federal da Paraíba (1993), mestrado em Sistemas e Computação pelo Instituto Militar de Engenharia (2000) e doutorado em Engenharia de Sistemas e Computação pela Universidade Federal do Rio de Janeiro (2006). Atualmente trabalha como engenheiro no Centro de Desenvolvimento de Sistemas (CDS) do Exército Brasileiro e é professor do Centro Universitário de Brasília – UniCEUB.

1 Introdução

O Sistema de Transações Financeiras baseado no protocolo Bitcoin (STFB) é vantajoso em comparação com sistemas de moedas tradicionais de e-cash e fiduciária (BITCOIN, 2016; FELD; SCHÖNFELD; MARTIN, 2014; MIERS et al., 2013; ARIAS; SHUN, 2013), particularmente por adotar dois princípios fundamentais: privacidade e segurança (FELD; SCHÖNFELD; MARTIN, 2014; ARIAS; SHUN, 2013).

Porém, não há visões detalhadas e globais de todas as atividades envolvidas, da dinâmica de seu funcionamento, dos produtos gerados e dos atores que participam em cada etapa do processo de negócio (BITCOIN FOUNDATION, 2015; BITCOIN, 2016). Esse cenário dificulta a análise do sistema sob variados vieses para poder-se inferir sobre aspectos relacionados a funcionalidades, usabilidade, desempenho, segurança, legalidade, economicidade e continuidade de negócio.

Nesse sentido, a construção e a disponibilização de artefatos técnicos de sistema constituem uma prática fundamental para estabelecer um veículo de comunicação entre os desenvolvedores, objetivando um entendimento comum a ser aplicado em todas as fases do ciclo de vida do sistema (DENNIS; WIXOM; ROTH, 2014; SOMMERVILLE, 2011). Sabe-se que a fase mais duradoura do ciclo de vida de um sistema é a de manutenção (SOMMERVILLE, 2011; LEHMAN, 1980). Nessa fase podem ser executados três tipos de manutenções: adaptativa – ajustes para adequação a alguma nova tecnologia implantada; corretiva – ajustes para correção de falhas; e evolutiva – criação de novas funcionalidades (SOMMERVILLE, 2011). O STFB está nessa fase.

Ante o exposto, este artigo tem o objetivo de apresentar a modelagem desse processo de negócio do STFB e detalhar seu processo primário Gerenciar Pagamento. Para tanto, são empregadas técnicas de Engenharia de Software (ES) e de Business Process Model and Notation (BPMN). Os modelos desenvolvidos permitem mapear problemas críticos do sistema, explicitando em quais etapas do processo de negócio eles exatamente incidem. Isso viabiliza principalmente a proposição mais efetiva de soluções e otimizações com vistas à maior robustez global do sistema.

O restante deste texto é organizado como descrito a seguir. A Seção 2 introduz conceitos fundamentais aqui adotados que visam a facilitar o entendimento do trabalho como um todo. A Seção 3 aborda os trabalhos relacionados. A Seção 4 apresenta a modelagem geral do processo de negócio do STFB bem como a modelagem do processo primário Gerenciar Pagamento. Por fim, a Seção 5 apresenta as conclusões finais e indicações de possíveis direcionamentos para trabalhos futuros.

2 Fundamentos

Neste trabalho, adotam-se os conceitos oriundos do BPMN (BUSINESS, 2011) mencionados a seguir:

a) processo de negócio: conjunto definido de atividades empresariais que representam os passos necessários para se alcançar um objetivo de negócio;

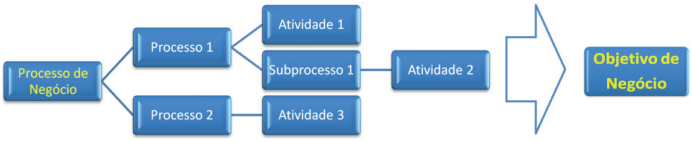
b) processo: descrição de uma sequência (ou fluxo) de atividades de uma organização com um objetivo a ser atingido;

c) atividade: trabalho realizado por uma organização dentro de um processo de negócio;

d) subprocesso: um processo que está incluído dentro de outro processo.

Como exemplo, a Figura 1 apresenta um esquema hierarquizado desses conceitos, em que se pode notar que o processo de negócio representado é o conjunto das atividades 1, 2 e 3 para se alcançar o objetivo de negócio.

Figura 1— Esquema hierarquizado de conceitos segundo o BPMN.



Fonte: Do autor.

Ainda, segundo o Guia BPM CBOK versão 3.0 (GUIA, 2013; LEHRMAN, 1980), os processos principais de uma área de negócio subdividem-se em:

a) primários - agregam valor diretamente ao cliente. Também chamados de essenciais ou finalísticos. Constroem a percepção de valor pelo cliente por estarem diretamente relacionados ao consumo do produto ou serviço;

b) de apoio - dão suporte a qualquer processo principal. Agregam valor a qualquer processo, inclusive a outros processos de apoio;

c) gerenciais - possibilitam medir, monitorar, controlar atividades e administrar o presente e o futuro do negócio. São necessários para assegurar que a organização opere de acordo com seus objetivos e metas de desempenho.

Por fim, a seguir são apresentadas algumas definições relacionadas à definição mais ampla do STFB:

a) *prova de trabalho*: função matemática que emprega esforço computacional para se encontrar uma nova cadeia de blocos de bitcoins válidos (NIELSEN, 2013; NAKAMOTO, 2008);

b) função de desafio de esforço computacional: também chamada de função *prova de trabalho* (NAKAMOTO, 2008);

c) protocolo misturador: protocolo para melhorar o serviço de anonimato onde utilizam-se moedas de múltiplos usuários, misturam-as por meio de entidades confiáveis que utilizam-se de criptografia e apresentam-as em uma única denominação aos usuários (BARBER et al., 2012);

d) revisão de histórico: obtenção de informações referentes às operações de bitcoins por meio de rastreamento de ações realizadas pelos usuários em cadeias de blocos bitcoins válidos (NAKAMOTO, 2008);

e) cadeia de blocos: sequência de blocos de bits que são agrupados formando elos em cadeias (NAKAMOTO, 2008);

f) ataques de *malware*: ações maliciosas realizadas por usuários, por meio de *softwares* específicos, visando obter vantagens de forma fraudulenta (BARBER et al., 2012);

g) chaves privadas e públicas: par de chaves criptográficas utilizadas em sistemas assimétricos de criptografia (BARBER et al., 2012);

h) moeda bitcoin: moeda eletrônica, não fiduciária, em uso no Sistema Bitcoin (NAKAMOTO, 2008);

i) mineração: processo de obtenção de moedas bitcoins pelos usuários mineradores ao realizarem provas de trabalhos (NIELSEN, 2013; NAKAMOTO, 2008);

j) sistemas autônomos: coleção de prefixos de roteamento conectados pelo Protocolo Internet (IP). Têm controle de um ou mais operadores de rede que apresentam uma política comum e claramente definida de roteamento para a Internet (RFC 1930, 1986; FELD; SCHÖNFELD; MARTIN, 2014);

k) carteira: aplicativo *web* utilizado pelos usuários no gerenciamento de suas moedas bitcoins (NIELSEN, 2013; NAKAMOTO, 2008);

l) moeda fiduciária: moeda que tem suporte governamental para sua emissão, circulação e realizações de transações financeiras. Não é lastreada a nenhum metal (ouro, prata) e não tem nenhum valor intrínseco. Seu valor advém da confiança (fidúcia, do latim *fidere*) que as pessoas têm de quem emitiu o título. Pode ser uma ordem de pagamento (cheques, por exemplo), títulos de crédito, notas promissórias, entre outros (FIAT MONEY, 2016);

m) processo Bitcoin: conjunto de atividades manuais e automatizadas utilizadas pelos usuários no gerenciamento de moedas bitcoins, tais como aquisição, disponibilização e circulação eletrônica (NIELSEN, 2013; BPM CBOK, 2011; NAKAMOTO, 2008);

n) sistema Bitcoin: processos automatizados utilizados pelos usuários no gerenciamento de moedas bitcoins (BPM CBOK, 2011; NAKAMOTO, 2008);

o) taxa de incentivo: percentual, em bitcoins, disponibilizados pelos usuários aos mineradores para proporcionar-lhes maior prioridade na realização de suas operações com bitcoins (NAKAMOTO, 2008).

3 Trabalhos relacionados

O protocolo Bitcoin foi originalmente proposto por Satoshi Nakamoto (2008). O autor retrata a filosofia e o mecanismo geral de funcionamento, os conceitos técnicos aplicados e a infraestrutura de *software* e de rede utilizada. Destaca-se, em especial, a necessidade do uso de um servidor de carimbo de tempo para gerar a *prova de trabalho* na ordem cronológica das transações realizadas.

Adam Back (2002) menciona que o Bitcoin emprega o conceito de *hashcash* para prevenir-se contra abusos de *spam* de mensagens eletrônicas e geradores automáticos de mensagens. Esse mecanismo foi implementado em uma função de desafio de esforço computacional chamada de *hashcash CPU cost-function*. Por sua vez, Barber et al. (2012) sugerem reformulações e melhorias no sistema Bitcoin, apresentando o protocolo misturador *fail-safe* para proteção contra ataques de revisão de histórico em cadeia de blocos. Os autores apresentam alguns problemas do Bitcoin que merecem mais investigação como, por exemplo, ataques de *malware* para roubo de chaves privadas dos seus usuários.

Para Arias e Chun (2013), o Bitcoin tornou-se popular devido a suas duas características mais distintivas: a) o seu fornecimento é ditado por uma fórmula matemática pré-programada que foi projetada para ser imune à política ou ao erro humano; e b) permite total anonimato/privacidade nas transações. Eles ressaltam que o mecanismo de armazenamento da moeda *bitcoin* é associado ao anonimato dos usuários em suas transações financeiras. Na sequência, Feld, Schönfeld e Martin (2014) apresentam uma abordagem sobre a rede Bitcoin

peer-to-peer (P2P) com foco especial sobre a sua distribuição entre *sistemas autônomos* distintos. Os autores examinam a rede P2P do Bitcoin considerando o tamanho da rede, o número de clientes e a distribuição da rede entre sistemas autônomos. Os resultados obtidos levam a conclusões quanto à resiliência do ecossistema Bitcoin, a univocidade da cadeia de bloco que utiliza, e a propagação e a verificação dos blocos de transações.

Laurie (2015) discorre sobre a criação de consenso em grupos abertos e em constantes alterações de seus membros. Isso é tido como um problema ainda sem solução. O consenso a que se refere é o que dá credibilidade na aplicação das regras para mineração. A questão reside exatamente em não se conhecer verdadeiramente cada um dos nós. Isso para possibilitar calcular a quantidade de nós para aplicação do consenso no reconhecimento da criação de moedas para entrar em circulação, o que feriria o princípio de anonimato adotado na filosofia do Bitcoin.

García Chávez e Silva Rodrigues (2015) apresentam uma proposta de algoritmo que pode melhorar significativamente o desempenho do processo de mineração de Bitcoin. Os autores retratam que há necessidade de uma melhoria da eficiência dos computadores de mineração e a redução das desvantagens quanto aos momentos de insucesso durante os saltos até encontrar dinamicamente um *pool* de mineiros mais eficiente. Já Eduardo Pazmiño e Silva Rodrigues (2015) discutem o tempo necessário para a verificação de uma transação no Sistema Bitcoin e propõem a divisão da base de dados considerando o uso das máquinas locais do cliente.

Um fator negativo ao sistema Bitcoin é a questão de que o número de *bitcoins* em circulação e de transações que a utilizam ser muito menor, se comparado ao que poderia ser (BITCOIN, 2016). Assim, eventos relativamente pequenos, trocas ou atividades de negócio podem afetar significativamente o seu preço de mercado. Ressalta que desenvolvedores do Bitcoin estão melhorando o *software*, mas sem considerarem mudanças no seu protocolo. Por fim, Nicholas Roth (2015) aborda a visão de Sistema de Sistemas (SoS) e insere o Sistema Bitcoin no Sistema de Sistemas Financeiros. Conceituam-se os elementos estruturais e comportamentais chaves para o SoS Bitcoin, incluindo o núcleo Bitcoin de rede e serviços que são construídos a partir dele. Para tanto, utiliza a Linguagem de Modelagem de Sistemas (SysML), onde apresentam-se vários Diagramas de Classes (SOMMERVILLE, 2011) e a correlação dos componentes do SoS Bitcoin.

4 Modelagem do Bitcoin

4.1 Atores e entidades externas

Atores de um processo têm responsabilidades, de acordo com seus papéis, na execução direta daquele processo do qual é participante (BPM CBOK, 2011). Entidades Externas (BPM CBOK, 2011), por sua vez, não participam de nenhum processo, mas se beneficiam indiretamente pela execução deles por seus atores. O Quadro 1 apresenta os atores e a entidade externa do Processo Bitcoin, bem como seus respectivos papéis. Membros podem ser acrescidos ou eliminados do processo.

Quadro 1— Atores e Entidade Externa do Processo Bitcoin

Nome	Categoria	Papel/Encargo
Usuário	Ator	Pessoa física que utiliza o Bitcoin para realizar pagamentos de bens e/ou serviços por meio de bitcoin. Realiza transações de compra de bitcoins com Lojistas ou Mineiros.
Empresa	Ator	Pessoa jurídica que utiliza o Bitcoin para comercializa bens e/ou serviços e aceita pagamentos por meio de bitcoins.
Mineiro	Ator	*Hardware* utilizado pelo Bitcoin para gerar moedas bitcoins, ao resolverem a função *prova de trabalho*. Validam transações de usuários que transitam pela rede. Podem agrupar-se formando *pool* de mineiros.
Lojista	Ator	Pessoa física ou jurídica que utiliza o Bitcoin para fornecer serviços de compra/venda/transferência de bitcoins com os atores do Sistema Bitcoin e disponibiliza aplicativos para os atores gerenciarem suas *carteiras* (GARCÍA CHÁVEZ; SILVA RODRIGUES, 2015). Eventualmente Mineiros ou Cambistas poderão ser Lojistas.
Cambista	Ator	Pessoa física ou jurídica que utiliza o Bitcoin para realizar troca de moedas bitcoins por fiduciárias, aplicando a taxa de câmbio de mercado. Eventualmente Lojistas poderão ser Cambistas.
Gestor	Ator	Pessoa física responsável por conduzir as ações do Processo Bitcoin para alcançarem seus objetivos propostos. Participa como *decisor* nas ações direcionadas à evolução e melhorias do processo como um todo.
Desenvolvedor	Ator	Pessoa física, com habilitação técnica, responsável pela construção e correção da documentação técnica e código do produto de *software* do Sistema Bitcoin. Está envolvida diretamente em cada etapa do ciclo de vida, desde sua criação até a manutenção do Sistema Bitcoin. Constrói e disponibiliza melhorias do Sistema Bitcoin, de acordo com as metas de negócio definidas pelo Gestor.
Sistema Financeiro	Entidade Externa	Instituição financeira que não interage com o Sistema Bitcoin. Faz fronteira com o Processo Bitcoin como responsável pela emissão/transação de moedas fiduciárias utilizadas pelos Cambistas na troca de moedas bitcoins por moedas fiduciárias.

Fonte: Do autor.

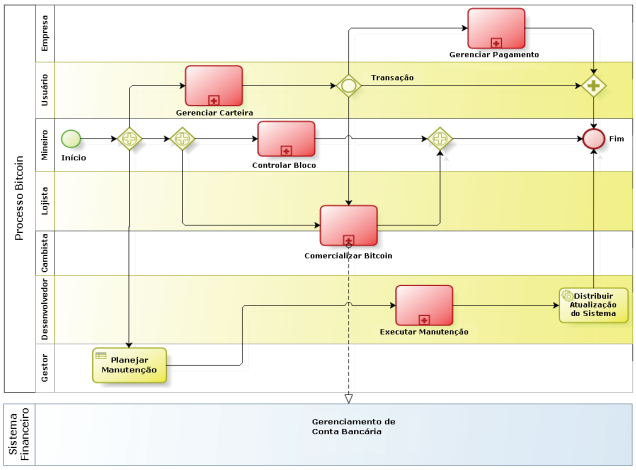
É oportuno destacar que atores de sistemas automatizados referem-se àqueles que executam alguma função interna do *software* que o constitui (DENNIS; WIXOM; ROTH, 2014; SOMMERVILLE, 2011). No Processo Bitcoin, os atores Desenvolvedor e Gestor não participam como atores do Sistema Bitcoin. Isso ocorre em virtude de os processos, dos quais eles participam, não serem automatizados. Essa situação é comum ocorrer em processos de negócio por variadas razões , por exemplo, a limitação de recursos financeiros a serem investidos pelos gestores e o desinteresse em sua automação por não agregarem valores efetivos (DENNIS; WIXOM; ROTH, 2014; SOMMERVILLE, 2011; BUSINESS, 2011).

4.2 Processos principais

Como o Sistema Bitcoin já está em produção (BITCOIN FOUNDATION, 2015) e também em fase de manutenção, a solução adotada para a coleta de informações necessárias à geração dos modelos a seguir apresentados foi o uso da técnica de *Engenharia Reversa* (SOMMERVILLE, 2011), com base nas informações coletadas pelo: a) estudo da literatura que trata do assunto; b) uso de aplicativos *web* disponíveis na Internet para transações com bitcoins, como *Coinbase* (COINBASE, 2016) e *Blockchain* (THE WORLD'S, 2016); c) Guia do Desenvolvedor (BITCOIN, 2015).

Os processos de negócio principais identificados para o Bitcoin são: *Comercializar Bitcoins*, *Gerenciar Pagamento*, *Gerenciar Carteira*, *Controlar Bloco* e *Executar Manutenção*. Esses representam as grandes áreas que englobam os principais serviços e/ou funcionalidades do Processo Bitcoin. A Figura 2 apresenta o modelo em sua visão ampla, em que constam esses processos principais.

Figura 2 – Modelo de Processos Principais do Bitcoin: Visão Geral



Fonte: Do autor.

Os processos assinalados na Figura 2, com um sinal de adição "+", indicam que possuem subprocessos integrantes. O Quadro 2 dispõe a especificação desses processos indicando: tipo (Gerencial, Apoio e Primário); descrição sumária; forma de execução (Automatizado e Manual) e atores participantes.

Quadro 2 – Especificação dos Processos Principais do Bitcoin

Nr	Processo Principal	Tipo	Breve Descrição	Forma de Execução	Atores
1	Comercializar Bitcoin	Primário	Contempla todos os processos relacionados à criação, compra e venda de Bitcoins entre os Atores do Processo Bitcoin. Faz fronteira com a Entidade Externa Sistema Financeiro nas operações de câmbio entre moedas bitcoin e fiduciárias.	A, M	Usuário Lojista Mineiro Cambista
2	Gerenciar Pagamento	Primário	Contempla todos os processos relacionados às transações de pagamentos e transferências de bitcoins entre os Atores do Processo Bitcoin.	A	Usuário Empresa Mineiro
3	Gerenciar Carteira	Primário	Contempla todos os processos relacionados ao gerenciamento de bitcoins pelas carteiras dos Atores do Processo Bitcoin.	A	Usuário
4	Controlar Bloco	Apoio	Contempla todos os processos referentes ao núcleo Bitcoin para controlar as transações efetuadas pelo sistema aplicando sua filosofia, protocolo e arquitetura para o tratamento de blocos e suas cadeias entre os nós de rede P2P.	A	Mineiro
5	Executar Manutenção	Gerencial e Apoio	Contempla os processos envolvidos na manutenção do Sistema Bitcoin, desde a identificação de erros até a disponibilização de *releases* atualizadas para entrada em produção.	A, M	Gestor Desenvolvedor
LEGENDA: (A) = Automatizado (M) = Manual					

Fonte: Do autor.

4.2.1 Processo Comercializar Bitcoin

Esse processo primário tem sua origem na criação da moeda para circulação em mercado e uso em transações de compra e venda de bitcoins pelos atores envolvidos. Essa cunhagem da moeda é feita pelos mineiros que, ao descobrirem novos blocos, por meio de mineração, têm creditados em suas carteiras, como taxa de incentivo, o valor de 25 BTC. Esse procedimento para creditar bitcoins, como incentivo aos mineradores, é realizado pelo processo de apoio *Controlar Bloco*.

O tempo médio para a cunhagem da moeda, isto é, para se encontrar um novo bloco na rede Bitcoin P2P, é de 10 minutos (BITCOIN, 2014). Esse tempo médio ainda é mantido em virtude da relação entre o aumento gradual da dificuldade na descoberta de novos blocos e o número crescente de mineiros atuantes.

Ainda, quanto à criação de novos blocos e, por conseguinte, quanto à cunhagem da moeda, tais blocos só são incorporados à cadeia de blocos se seu *hash* tiver um grau de dificuldade tal que atenda às exigências quanto ao valor esperado pelo consenso dos demais nós da rede P2P envolvidos na validação de blocos (BITCOIN, 2016; WHITE, 2015). Assim, para cada 2.016 blocos (BITCOIN, 2016; BITCOIN, 2014), a rede usa carimbos de tempos armazenados em cada cabeçalho do bloco para calcular o número de segundos decorridos entre a geração do primeiro e do último desses 2.016 blocos. O valor ideal (BITCOIN, 2016) é 1.209.600 segundos, o que equivale a aproximadamente duas semanas (BITCOIN, 2016).

Uma vez adquirida a moeda, ela é comercializada entre usuários e lojistas que compram BTC para realizarem suas transações de pagamentos ou simplesmente guardá-las como forma de investimento. A compra de bitcoins pode ter sua origem (BITCOIN, 2014) a partir de: uma pessoa (ator Usuário), uma casa de câmbio**,** ou em máquinas ATM (ator Cambista). Os procedimentos para a realização de operações de compra e venda de bitcoins são muito similares ao previsto no processo primário *Gerenciar Pagamento*, incluindo-se adaptações para adequar-se ao objeto da operação, ou seja, bitcoins.

A quantidade finita de bitcoins (21 milhões), prevista para a moeda, não é uma limitação do sistema. Transações poderão ser fragmentadas em subunidades menores que um bitcoin. Bitcoins podem ser divididos em até 8 casas decimais (0,00000001) e em unidades potencialmente ainda menores, se necessário no futuro, conforme o tamanho médio das transações diminuem (BITCOIN, 2009).

4.2.2 Processo Gerenciar Carteira

O processo primário *Gerenciar Carteira* possibilita a cada ator do Sistema Bitcoin criar uma carteira para gerenciar seu saldo de bitcoins, realizar transações de compra de produtos/serviços com empresas, que aceitam bitcoins como forma de pagamento, fazer transferência de valores bitcoins com outros atores, e a realização das demais transações financeiras normalmente encontradas nos sistemas tradicionais.

Há vários lojistas que disponibilizam esse serviço de carteiras, por exemplo, o *Blockchain* e o *Coinbase*. Outra função importante aos atores do sistema é poder converter bitcoins em moedas fiduciárias, onde alguns cambistas disponibilizam essa facilidade no próprio gerenciador de carteiras e praticam as taxas de câmbio de mercado. Nesse ponto, o Processo Bitcoin faz fronteira com a entidade externa Sistema Financeiro, que disponibiliza moedas fiduciárias para o processamento desse tipo de transação.

4.2.3 Processo Gerenciar Pagamento

A aquisição de bens e serviços, oriundos do ator Empresa, motiva a execução do processo primário *Gerenciar Pagamento*. As atividades integrantes desse processo possibilitam aos envolvidos poder verificar situações de pagamentos, como operações pendentes, vencidas, realizadas e estornadas.

O seu mecanismo de funcionamento é similar a outros *e-cash*, como o *Paypal* (WHITE, 2015), onde o credor verifica a efetivação da transferência de valores bitcoin, a título de pagamento, para posteriormente executar o serviço ou remeter o produto objeto da transação. Esse trâmite de informações é intermediado pelos mineiros, através da rede P2P, que exercem a função de validação das transações para dar credibilidade e segurança.

4.2.4 Processo Controlar Bloco

Como elemento-chave do Processo Bitcoin, o processo de apoio *Controlar Bloco* é a essência do sistema, e muitas vezes é chamado de núcleo Bitcoin. Sendo assim, esse processo é reutilizado pelos demais processos principais. Nele são executadas funcionalidades que implementam a filosofia do sistema, ou seja, o emprego de técnicas como *prova de trabalho*, *função hash*, geração de cadeia de blocos com uso de *árvore de Merkle* (NAKAMOTO, 2008), validação de blocos de transações financeiras, aplicação de algoritmos criptográficos de *chave pública* resultando em segurança nas transações e no anonimato dos envolvidos, a mineração de bitcoins, dentre outras atividades que o compõe.

Como bitcoins são criados a uma taxa decrescente e previsível, o número de novos bitcoins criados a cada ano é automaticamente reduzido pela metade, com o passar do tempo, até que a emissão seja completamente suspensa ao se atingir o total de 21 milhões de BTC previstos. Nesse ponto, os mineradores provavelmente serão suportados exclusivamente por numerosas pequenas taxas de transação.

4.2.5 Processo Executar Manutenção

Este processo de apoio, comentado no Guia Bitcoin (BITCOIN, 2015), carece de maiores esclarecimentos. Segundo a abordagem do Guia, o desenvolvimento e a manutenção do sistema ocorrem na forma de desenvolvimento colaborativo (GITHUB, 2016; BITCOIN, 2014), similar a outros produtos de *software* desenvolvidos em código aberto, onde são constituídas comunidades ou grupos organizados de desenvolvedores colaboradores.

Desenvolvedores trabalham em suas próprias árvores de manutenção (GITHUB, 2016) e submetem, a essa comunidade, as correções de erros quando prontas. Ao tratar-se de mudanças simples, triviais ou não controversas, um dos membros do grupo de desenvolvedores do Bitcoin simplesmente as submete para atualização do sistema.

Entretanto, quando a mudança é mais complexa ou potencialmente controversa, é solicitada, ao responsável pela correção, a iniciação de uma discussão do assunto em uma lista de *e-mail* de desenvolvedores. Caso haja consenso dos integrantes da lista de que a correção trata-se de uma boa solução, ela é tida como aceita para disponibilização aos usuários do sistema. Entretanto, desenvolvedores podem refazer e remeter novas submissões (GITHUB, 2016).

Como parte da árvore de manutenção do sistema, o *Branch Master* (GITHUB, 2016) é regularmente construído e testado, mas não é garantido ser completamente estável. Já *Tags* (GITHUB, 2016) são criadas, com regularidade, para indicar novas versões estáveis do Bitcoin. Ainda, os testes e revisões de código são considerados *gargalos* ao desenvolvimento, mesmo que sua execução seja realizada de forma automática, pois há mais requisições de mudanças do que a capacidade do grupo em poder rever e testar códigos em curto prazo. Isso compromete a qualidade do sistema.

O *Bitcoin Improvement Proposal* (BIP) é um documento de projeto para a introdução de recursos ou informações para o Bitcoin. Essa é a maneira padrão de comunicação de ideias uma vez que a manutenção do Bitcoin não tem uma estrutura formal (BITCOIN FOUNDATION, 2015).

Ainda sobre o processo *Executar Manutenção*, devem-se considerar os vários problemas já identificados para que, de forma criteriosa, sejam levados a efeito possíveis soluções a serem implementadas, sem comprometer a filosofia do sistema. A título de exemplo, o Quadro 3 apresenta alguns desses problemas, de forma reduzida, identificados na literatura.

Quadro 3— Problemas Identificados no Bitcoin

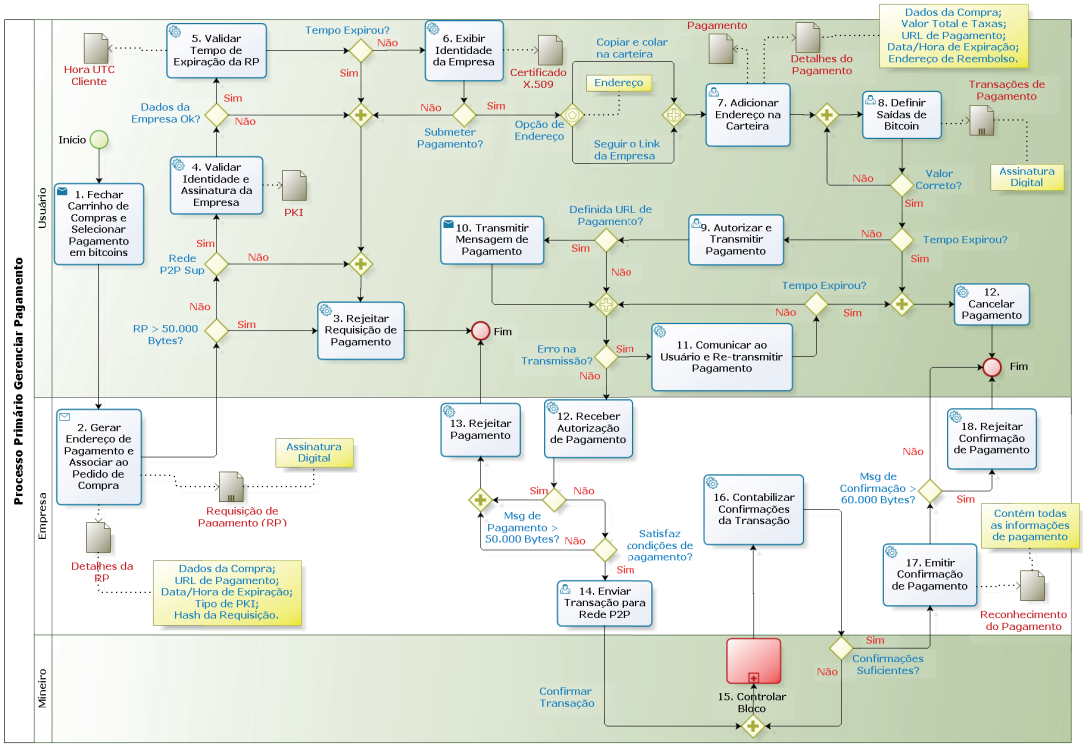
Processo Principal CONTROLAR BLOCO
Falta de implementação de uma capacidade que garanta menores custos de transação (ROTH, 2015); Comprometimento da segurança caso seja do conhecimento do usuário uma cadeia de blocos que contenha transações realizadas em *sites* comprometidos ou chaves públicas bem conhecidas, pois poderiam ser utilizados para descobrir informações de pessoas ou organizações, quebrando o anonimato preconizado pelo Sistema Bitcoin (ROTH, 2015); Aumento significativo do custo por transação devido ao valor dos bitcoins ter aumentado desproporcionalmente em relação ao número de transações (ROTH, 2015); Falta de informações aos engenheiros de *software* que integram sistemas com Bitcoin quanto ao comportamento e uso da função prova de trabalho e como ocorre a validação de transações (ROTH, 2015); Deflação do bitcoin em face da expiração de cunhagem da moeda e extinção de incentivo aos mineiros para manter o Bitcoin funcionando. Além disso, moedas com chaves públicas esquecidas/destruídas (moedas zumbis) não serão substituídas, reduzindo o dinheiro base (BARBER et al., 2012); Comprometimento da segurança, no futuro, impactada pela deflação do bitcoin, pois tende a se valorizar, incentivando fraudes. Extinguindo-se o incentivo para mineração reduzirá futuramente a dificuldade na criação de blocos em relação ao poder computacional, facilitando ataques de revisão de históricos (BARBER et al., 2012); Nós da rede podem verificar transações, porém este método simplificado pode ser enganado por transações fraudulentas enquanto o invasor continuar dominando a rede (NAKAMOTO, 2008).
Processo Principal GERENCIAR PAGAMENTO
O custo de uma transação bitcoin pode ser definido, mas cabe ao usuário determinar se o valor dos benefícios do sistema para ele vale a pena o custo adicional. Não há garantia de que o custo inerente seja menor do que um sistema tradicional, do mesmo modo que há uma garantia de que a transação é irreversível (ROTH, 2015); Falta de capacidade do beneficiário em poder verificar se um dos proprietários não passou duas vezes a mesma moeda. Solução: Introduzir uma Autoridade Central de Confiança (ACC) para verificar todas as transações (NAKAMOTO, 2008); Aumento significativo do custo por transação devido ao valor dos bitcoins ter aumentado desproporcionalmente em relação ao número de transações (ROTH, 2015).
Processo Principal EXECUTAR MANUTENÇÃO
Desinteresse dos atores do sistema em cientificarem-se de mudanças no protocolo e sua difusão ao resto da rede. Isso exigirá maior pró-atividade do grupo de desenvolvedores (ROTH, 2015); Falta de esforço direcionado à arquitetura do Bitcoin para lidar com as complexidades de nível SoS existentes atualmente (ROTH, 2015); Falta de informações no site da Fundação Bitcoin, já que considera mudanças no protocolo (BITCOIN FOUNDATION, 2015), sobre como as mudanças são desenvolvidas, amadurecidas, testadas e implementadas (ROTH, 2015).
Processo Principal GERENCIAR CARTEIRA
a) nada a considerar.
Processo Principal COMERCIALIZAR BITCOIN
a) nada a considerar.

Fonte: Do autor.

4.3 Processo Primário Gerenciar Pagamento

Como disposto no Quadro 2, este processo tem a participação dos atores Usuário, Empresa e Mineiro. Ele se destina ao controle de pagamentos em bitcoins. A Figura 3 apresenta o modelo detalhado contendo as atividades integrantes.

Figura 3 – O Modelo do Processo Primário Gerenciar Pagamento – Nível 1



Fonte: Do autor

Ao analisar a Figura 3, há pontos de controle no fluxo da execução das atividades, assinalados por um losango que implementam regras de negócio para o processo em questão. A leitura do modelo representado pode ser entendida como uma sequência de ações que são desencadeadas para o gerenciamento de pagamentos pelo Sistema Bitcoin. A seguir discorre-se sobre detalhes dos passos seguidos para a execução das atividades do modelo da Figura 3, onde se destacam algumas técnicas utilizadas nesse processo do Bitcoin.

Inicialmente, o cliente (Usuário) efetua a compra de produto/serviço do comerciante (Empresa), pelo *site* da Internet, fecha o carrinho de compras, opta pagar com bitcoins e submete ao Comerciante. Este, por sua vez, identifica o pedido de compra e a forma de pagamento do cliente. Por meio de sua carteira Bitcoin, associa seu endereço ao pedido de compras e cria uma mensagem de Requisição de Pagamento (RP) contendo: dados da compra, URL de pagamento do Comerciante, data/hora de expiração da RP, tipo de sistema de chave pública (PKI) utilizada, e *hash* da RP. Assina a RP e remete ao cliente.

A carteira do cliente verifica se a mensagem que contém a RP é menor que 50.000 bytes, se a rede suporta tal transação, se a identidade e assinatura do Comerciante são corretas, e se a RP não expirou seu prazo. Em caso de não conformidade em alguma dessas verificações, a RP é rejeitada. O cliente, por meio de sua carteira, visualiza a identidade do Comerciante, ao qual teve a transação de compra realizada, e lhe é solicitado que copie o endereço de pagamento ou siga o *link* que contém tal endereço a ser inserido na carteira do cliente para efetivação do pagamento.

Após a definição de endereço acima, a carteira do cliente gera uma Mensagem de Pagamento (MP) contendo: dados da compra, valor e taxas a serem pagas, URL de pagamento, data/hora de expiração da MP e endereço de reembolso (em caso de estorno). O cliente define quais saídas de bitcoin disponíveis deseja utilizar para pagar a compra, autoriza o pagamento e transmite a MP ao Comerciante. Antes dessa transmissão da MP, a carteira do cliente verifica: a) se a soma dos valores das saídas bitcoin é igual ao valor da compra, pois não havendo essa coinci-

dência de valores, é solicitada a devida correção; e b) se a MP não expirou seu prazo (caso contrário, o pagamento é cancelado).

Realizadas essas verificações de valores e regras de negócio, a MP é transmitida ao Comerciante. No caso de o Comerciante ainda ter informado a URL de pagamento, outra mensagem é encaminhada a ele comunicando a execução do pagamento. Em caso de erro na transmissão, é solicitado ao cliente a retransmissão da MP, seguindo as mesmas condições indicadas no parágrafo anterior.

O Comerciante, por meio de sua carteira, recebe a MP do cliente e verifica se a MP é menor que 50.000 bytes e se atende às condições de pagamento, do contrário a MP é rejeitada. Satisfeitas essas condições, a transação, referente ao pagamento, é submetida aos Mineiros, via rede Bitcoin P2P, para sua confirmação e retorno.

Como forma de controle dessa etapa do processo, a carteira do Comerciante contabiliza as respostas de confirmação da transação, oriunda dos mineiros, e ao se obter um número suficiente, normalmente superior a cinco, emite um recibo de pagamento. Então, é gerada uma mensagem de Confirmação de Pagamento (CP), que contém todas as informações existentes na RP e na MP, e transmitida ao cliente. Se a CP for maior que 60.000 bytes, esta será automaticamente rejeitada.

5 Conclusões e trabalhos futuros

Este artigo teve o objetivo de apresentar o processo de negócio do Bitcoin e detalhar um de seus processos primários, *Gerenciar Pagamento*, com emprego de técnicas da Engenharia de *Software* e *Business Process Model and Notation*.

O detalhamento desse processo primário, aqui apresentado, permite: a) entender como é seu mecanismo de funcionamento; b) identificar que tecnologias foram aplicadas em cada etapa do processo; e c) possibilitar, por exemplo, a identificação de impactos no Processo Bitcoin quando ocorrer mudanças de um determinado processo principal do Bitcoin.

Como trabalho futuro, sugere-se estender a modelagem aqui realizada para contemplar os demais processos principais do Bitcoin. Isso permitirá ampliar a coleta de informações inerentes ao sistema Bitcoin em todos os processos aqui identificados e, com isso, uma visão mais refinada que redunda na a possibilidade da proposição de soluções e otimizações com vistas à maior robustez global do sistema.

Referências

ARIAS, Maria A.; SHUN, Yongseok. There are two sides to every coin: even to the Bitcoin, a virtual currency. *The Regional Economist*, St. Louis, Jul. 2013.

BACK, Adam. *Hashcash-A denial of service counter-measure*. 2002. Available in: <http://www.hashcash.org/papers/hashcash.pdf>. Accessed: 4 Feb. 2016.

BARBER, Simon et al. *Bitter to better-how to make bitcoin a better currency*. 2012. Available in: <https://crypto.stanford.edu/~xb/fc12/bitcoin.pdf>. Accessed: 4 Feb. 2016.

BITCOIN Developer Guide: Find detailed information about the Bitcoin protocol and related specifications. 2015. Available in: <https://bitcoin.org/en/developer-guide>. Accessed: 16 Jun. 2016.

BITCOIN FOUNDATION. [*Home Page*]. 2015. Available in: <https://bitcoinfoundation.org/>. Accessed: 16 Jun. 2016.

BITCOIN help: What is Bitcoin? Available in: <https://bitcoinhelp.net>. Accessed: 16 Jun. 2016.

BITCOIN. *Frequently Asked Questions*. [2009?]. Available in: <https://bitcoin.org/pt_BR/faq>. Accessed: 16 Jun. 2016.

BITCOIN. In: Wikipedia: the free encyclopedia. Florida: Wikimedia Foundation, 2016. Available in: <https://en.bitcoin.it/wiki/Main_Page>. Acessed: 16 Jun. 2016.

BUSINESS Process Model and Notation (BPMN) Version 2.0. 2011. Available in: <http://www.omg.org/spec/BPMN/2.0/PDF>. Accessed: 16 Jun. 2016.

COINBASE. *Get started with Bitcoin*. 2016. Available in: <https://www.coinbase.com>. Accessed: 16 Jun. 2016.

DENNIS, Alanis; WIXOM, Barbara Haley; ROTH, Roberta M. *Análise e projeto de sistemas*. 5. ed. Rio de Janeiro: LTC, 2014.

EDUARDO PAZMIÑO, J.; SILVA RODRIGUES, C. K. Simply dividing a Bitcoin network node may reduce transaction verification time. *The SIJ Transactions on Computer Networks & Communication Engineering*, Tiruppur, v. 3, n. 2, p. 17-21, 2015.

FELD, Sebastian; SCHÖNFELD, Mirco; MARTIN, Werner. Analyzing the deployment of Bitcoin's P2P network under an AS-level perspective. *Procedia Computer Science*, Amsterdam, v. 32, p. 1121-1126, 2014.

FIAT MONEY. In: Wikipedia: the free encyclopedia. Florida: Wikimedia Foundation, 2016. Available in: <https://en.wikipedia.org/wiki/Fiat_money>. Accessed: 16 Jun. 2016.

GARCÍA CHÁVEZ, Juan J.; SILVA RODRIGUES, C. K. da. A simple algorithm for automatic hopping among pools in the Bitcoin Mining Network. *The SIJ Transactions on Computer Networks and Communication Engineering,* Tiruppur, v. 3, n. 2, p. 22-27, 2015.

GITHUB. *Bitcoin*. Available in: <https://github.com/bitcoin>. Accessed: 16 Jun. 2016.

GUIA para gerenciamento de processos de negócio corpo comum de conhecimento BPM CBOK v 3.0. [S.l]: ABPMP Brasil, 2013. Disponível em: <http://www.abpmp.org/resource/resmgr/Docs/ABPMP_CBOK_Guide__Portuguese.pdf./>. Acesso em: 16 jun. 2016.

HAWKINSON, J. *As guidelines for creation, selection, and registration of an autonomous system*. 1986. Available in: <http://www.ietf.org/rfc/rfc1930.txt>. Accessed: 16 Jun. 2016.

LAURIE, Ben. *Decentralized currencies are probably impossible but let's at least make them efficient*. 2015. Available in: <http://www.links.org/files/decentralised-currencies.pdf>. Accessed: 16 Jun. 2016.

LEHMAN, Meir M. Programs, life cycles, and laws of software evolution. *Proceedings of the IEEE*, EUA, v. 68, n. 9, p. 1060-1076, 1980.

NAKAMOTO, Satoshi. Bitcoin: *A Peer–to–peer Electronic Cash System*. 2008. Available in: <http://www.bitcoin.org/bitcoin.pdf>. Accessed: 16 Jun. 2016.

NIELSEN, Michael. *How the Bitcoin protocol actually works*. 2013. Available in: <http://www.michaelnielsen.org/ddi/how-the-bitcoin-protocol-actually-works/>. Accessed: 16 Jun. 2016.

ROTH, Nicholas. An architectural assessment of Bitcoin using the systems modeling language. *Procedia Computer Science*, Amsterdam, v. 44, p. 527-536, 2015.

SOMMERVILLE, Ian. *Software engineering*. 9. ed. São Paulo: Pearson, 2011.

THE WORLD'S Most Popular Bitcoin Wallet. 2016. Available in: <https://www.blockchain.com>. Acessed: 16 Jun. 2016.

WHITE, Lawrence H. The market for cryptocurrencies. *The Cato Journal*, Chicago, v. 35, n. 2, p. 383-402, Spring/Summer, 2015. Available in: <http://www.cato.org/pubs/journal/index.html>. Accessed: 16 Jun. 2016.