A Proposal to Automate the Public Budgetary and Financial Management of Brazil through the Blockchain / Bitcoin System

Uma Proposta para Automatizar a Gestão Pública Orçamentária e Financeira do Brasil usando o Sistema Blockchain / Bitcoin

Carlo Kleber da Silva Rodrigues[1], Paulo Caetano da Silva[2], Mauricio Codesso[3]

[1]Centro de Matemática, Computação e Cognição (CMCC) – Universidade Federal do ABC – Santo André, SP – Brazil

[2]Programa de Pós-Graduação em Sistemas e Computação – Universidade Salvador – Salvador, BA – Brazil.

[3]Rutgers Business School – Newark – NJ – USA.

carlo.kleber@ufabc.edu.br, paulo.caetano@unifacs.br, mmcodesso@gmail.com

Abstract. *This article proposes the deployment of the Bitcoin system for automating the budgetary and financial public management of the country Brazil. To this end, an overall view of the Bitcoin system is firstly presented. It then follows a brief explanation of the existing brazilian model of budgetary and financial management. We then elaborate on how to do this automation, highlighting the main arising benefits. Finally, we discuss over the computational environment Ethereum, where this automatization may be implemented in practice. From the results and discussions, it is possible to conclude about the technological strength of the Bitcoin system and conjecture about the significant decrease at the bureaucracy of the budgetary and financial management process currently in use. Future avenues within this research area appear at the end of this article.*

Resumo. *Este artigo propõe o emprego do sistema Bitcoin para automatizar a gestão pública orçamentária e financeira do Brasil. Para este fim, inicialmente se apresenta uma visão geral do sistema Bitcoin. Em seguida, segue-se uma breve explicação do modelo de gestão orçamentária e financeira vigente. Na sequência, explica-se como realizar a automatização proposta, ressaltando os principais benefícios decorrentes. Finalmente, discorre-se sobre o ambiente computacional Ethereum, onde a automatização pode ser implementada na prática. A partir dos resultados e discussões, é possível concluir-se sobre a robustez tecnológica do sistema Bitcoin e conjecturar sobre a diminuição da burocracia presente no modelo de gestão vigente. Sugestões para pesquisas futuras aparecem ao fim deste artigo.*

1. Introdução

Os sistemas de pagamentos eletrônicos têm evoluído para tornar as transações financeiras do cotidiano cada vez mais práticas para todos na sociedade. Isso implica principalmente em tentar assegurar que essas transações sejam realizadas de maneira fácil, rápida e segura, permitindo a obtenção de produtos, incluindo bens e serviços, das mais distintas naturezas.

Em especial, ao se pensar em transações envolvendo recursos públicos financeiros, a facilidade de realização, a rapidez e a segurança das transações precisam ser acompanhadas pela imperiosa necessidade de transparência do processo do negócio. Nesse sentido, é mister haver ferramentas que possibilitem execução e controle efetivos para garantir que o produto que se obtém é de fato o que se expressa formalmente quando da aprovação de sua obtenção. Tempo de entrega, custo, qualidade, confiabilidade e, principalmente, atendimento da real necessidade, identificada no início do processo, são alguns dos parâmetros a serem observados neste contexto (IKA, 2009; HENDERSON, 2004; ALVES et al., 2013).

Sob o modelo de gestão pública vigente, toda a despesa gerada é classificada por meio de um sistema de códigos numéricos (FEIJÓ et al., 2014). Mais especificamente, a classificação da despesa na *Execução Orçamentária* é feita pela agregação de seis dígitos, representando categoria econômica, grupo de natureza da despesa, modalidade de aplicação, e elemento de despesa, conforme identificação e conceituação previstas em lei. Para a *Execução Financeira* da despesa, a classificação orçamentária é ainda complementada com mais dois dígitos que representam conjuntamente o subelemento de despesa (BRASIL, 2015).

Em que pese a importância do detalhamento de despesa preconizado, é razoável conjecturar que o planejamento, a execução e o controle orçamentário e financeiro tornam-se burocráticos, pouco flexíveis e de difícil gestão. Essa caracterização é ainda evidenciada ao considerar-se o fato de que os processos se desenvolvem majoritariamente ao longo de um período que se estende por quatro anos, correspondendo ao tempo de mandato de um governo eleito, e envolvem atores independentes como, por exemplo, funcionários públicos e privados, empreiteiros e parlamentares. Nesse cenário, a possibilidade de conflito de interesses e a digressão com respeito aos objetivos originais são propícias de ocorrer.

No entanto, o intrincamento resultante das questões anteriores pode ser atenuado pela automatização do modelo vigente através do sistema de pagamento eletrônico *Bitcoin* (DYHRBERG, 2016; LUTHER 2015; RODRIGUES, 2017; SILVA e RODRIGUES, 2016). Este sistema envolve muito mais que dinheiro e pagamentos, incluindo uma infinidade de propriedades associadas a transações. Ele permite a implementação de uma moeda inteligente e, assim, a automatização do fluxo de transferências de pagamentos sob quaisquer regras desejadas (WEUSECOINS, 2016).

Por exemplo, é possível uma programação de um montante de recursos financeiros de forma que ele voltará automaticamente para o emissor se o receptor não o utilizar depois de um certo período de tempo, evitando desperdícios e perdas de fundos por não utilização tempestiva. Ainda, podem-se controlar despesas diversas da mesma maneira, por exemplo, programando orçamentos específicos para salários, materiais de consumo ou permanentes, equipamentos e serviço de manutenção. Nesse sentido, os montantes correspondentes a custeio ou a investimento passam a ser dedicados para cada área e não podem ser utilizados de forma distinta, evitando o desvio de finalidade ou a denominada improbidade administrativa (FEIJÓ et al., 2014; BRASIL, 2015).

Neste contexto, cabe indagar: Não podemos usar a tecnologia que já conhecemos? A resposta a essa pergunta é que não podemos usar a tecnologia tradicional e continuar digitalizando transações. Não é encontrada uma solução confiável para criar, promulgar, verificar, armazenar e proteger contratos digitais. Até que tal solução se apresente, a tecnologia *blockchain* parece ser uma solução com grandes benefícios e talvez sem alternativas. Três propriedades de soluções digitais têm sido muito difíceis, ou até

impossíveis, antes da *blockchain* (LANTMÄTERIET et. al., 2017), as quais são descritas a seguir:

1) **Unidades digitais impossíveis de copiar –** Para um banco central que está prestes a emitir moeda para o mercado, pode-se facilmente identificar algumas preocupações. É óbvio que uma delas é da maior importância: as cédulas devem ser muito difíceis de copiar. O mesmo deve ser verdadeiro para o dinheiro digital. Se um banco central emitir dinheiro em formato digital, é crucial que ele não possa ser copiado. No entanto, tal característica do mundo digital não existiu até recentemente. O *Bitcoin* foi o primeiro a resolver este problema de "duplicação". Muitos bancos centrais e bancos comerciais já estão considerando a oportunidade de emitir dinheiro digital usando *blockchain* ou com uma outra tecnologia de contabilidade distribuída. Nenhum deles está procurando fazer isso com qualquer outra tecnologia. Até onde sabemos, a *blockchain* é a única solução que está sendo investigada por esse crescente grupo de bancos centrais e bancos comerciais. Talvez a principal razão para isso seja a possibilidade de criar unidades digitais transferíveis, que possuem características que sejam impossíveis de copiar, ou ao menos próximo disto.

2) **Arquivos digitais que não podem ser manipulados -** Há outra propriedade, exceto a possibilidade de copiar, que a TI tradicional ainda não resolveu. É muito difícil saber se um arquivo digital, foto, contrato etc. foi manipulado. Como exemplo, por lei qualquer alteração na contabilidade de uma empresa deve ser registrada com uma notificação de quem fez a alteração, por que foi feita e quando foi feita. O problema com essa regra é que é impossível auditar. Uma pessoa de TI experiente pode fazer alterações no registro da contabilidade que não podem ser detectadas, ou dificilmente poderão. Não há nenhuma maneira prática para um gerente ou a organização, um contador ou a autoridade fiscal saber quem fez essas mudanças e quando elas foram feitas, ou perceber que qualquer mudança foi feita. Entretanto, tecnologias modernas tornaram possível monitorar as atualizações. Com a *blockchain* é possível se certificar de que um arquivo digital ainda é o mesmo de quando foi registrado pela primeira vez no blockchain. A tecnologia de *hashing* e a *blockchain* são as únicas tecnologias conhecidas que pode fazer isso. Se queremos representar digitalmente contratos, é de suma importância que sejam impossíveis, ou pelo menos muito difíceis, de manipular. A *blockchain*, até o momento, é a solução mais confiável para isso.

3) **Processos digitais que não podem ser manipulados -** Um terceiro problema resolvido pela *blockchain* é proteger um processo. O exemplo mais discutido de tal processo é o financiamento do comércio, em que uma sequência de atores precisa confirmar o que está fazendo em vários estágios do acordo. Eles têm que assumir a responsabilidade pelas mercadorias que estão sendo enviadas e confirmar o processo para os atores em toda a cadeia de transporte. Garantir um processo também é valioso em um contrato, é importante que todas as partes envolvidas estejam confiantes de que todas as outras partes estão assinando o contrato em uma ordem aceitável. É muito importante evitar ou detectar qualquer manipulação dos processos em que produtos estão envolvidos, antes de causar qualquer dano.

Segundo Marc Andreesen, a consequência prática de resolver esse problema é que o *Bitcoin* nos dá, pela primeira vez, uma forma de um usuário da Internet transferir uma propriedade exclusiva de propriedade digital para outro usuário da Internet, garantindo que a

transferência seja segura e protegida. Todos sabem que a transferência ocorreu e ninguém pode contestar a legitimidade da transferência[1].

Ante o exposto, este artigo tem o objetivo de propor e discutir o emprego do sistema *Bitcoin* para automatizar a gestão pública orçamentária e financeira do Brasil. Cabe destacar a importante interdisciplinaridade contida neste objetivo por considerar a proposta de utilização de um sistema tecnológico de concepção inovadora, e ainda em exploração, para o aperfeiçoamento de um tradicional modelo de gestão administrativo, orçamentário e financeiro.

Para alcançar-se este objetivo, inicialmente apresenta-se uma visão geral do sistema *Bitcoin*. Logo depois, comenta-se sobre o modelo vigente de gestão orçamentária e financeira pública do Brasil. Na sequência, realiza-se uma discussão sobre o que automatizar nesse modelo e as vantagens decorrentes. Finalmente, faz-se uma breve explicação do ambiente computacional *Ethereum* (WOOD, 2015), onde a automatização proposta pode ser implementada na prática.

É importante ressaltar o ineditismo deste artigo, por ser salvo melhor juízo, o primeiro trabalho que formalmente, sob vieses científico e tecnológico, aborda a possibilidade de emprego de um sistema eletrônico de pagamento baseado em criptomoedas na administração pública do Brasil.

O restante deste texto está estruturado conforme descrito a seguir. A Seção 2 traz os trabalhos relacionados. A Seção 3 explica o sistema *Bitcoin*. A Seção 4 traz uma discussão visionária sobre o emprego desse sistema para a automatização do modelo de gestão em comento e explora brevemente o ambiente *Ethereum*, com foco na possibilidade de implementação prática dessa automatização. Finalmente, conclusões gerais e trabalhos futuros estão na Seção 5.

2. Trabalhos Relacionados

A despeito dos inúmeros trabalhos sobre gestão pública orçamentária e financeira, entende-se que é suficiente a menção aqui apenas daqueles mais recentes que tratam sobre o modelo de gestão e, simultaneamente, trazem subsídios para permitir conjecturar-se sobre a importância da automatização dessa gestão em si.

A seleção dos trabalhos, comentados a seguir, ocorreu para prover ao leitor, no contexto da gestão pública orçamentária e financeira, uma visão das principais constatações já feitas sobre modelos de gestão, a identificação das necessidades de aperfeiçoamento e, por fim, o entendimento do atual estado da arte nessa área de pesquisa.

Bairral, Coutinho e Silva, e Alves (2010) analisaram o nível de transparência pública nos relatórios de gestão anuais de entidades públicas federais e os incentivos (político, institucional, governamental, social e financeiro) que podem afetar a divulgação da informação pública. Para tanto, foi construído um Índice de Transparência Pública Federal (ITPF), baseado em estudos internacionais, de modo a verificar o nível de divulgação da informação pública apresentado nos relatórios de gestão anuais e os correspondentes incentivos que afetam essa divulgação.

[1] Marc Andreessen, Why Bitcoin matters, New York Times, January 21, 2014

Os resultados alcançados apontaram um baixo nível de transparência pública nos relatórios de gestão (48%), deficiências na divulgação obrigatória (80%) e baixa aderência às práticas de evidenciação voluntária (19%). Sobre os incentivos para a divulgação, se observou uma relação positiva entre o tipo de entidade, acessibilidade e demografia de pessoal com o índice de transparência pública, enquanto a burocracia pública mostrou uma relação negativa. Já o porte, tamanho do núcleo de gestão, receita orçamentária e dependência federal não influenciaram a divulgação da informação pública nos relatórios.

De Souza et al. (2013) analisaram o grau de transparência relacionado à gestão orçamentária e financeira dos municípios mais populosos do Estado do Rio Grande do Norte (RN). Para atingir esse objetivo, foram selecionados os municípios do RN que possuíam mais de 50.000 habitantes, o que resultou em uma amostra de oito municípios, a saber: Natal, Mossoró, Parnamirim, São Gonçalo do Amarante, Macaíba, Ceará-Mirim, Caicó e Açu. A metodologia para estabelecer um *ranking* de transparência dos municípios considerou variáveis como execução orçamentária, classificação orçamentária, contratos, séries históricas, possibilidade de *download* de documentos e facilidade de navegação no sistema.

Os resultados revelaram que o município de melhor índice de transparência, entre os oito analisados, foi o de Natal, com 79% da pontuação possível, seguido por Parnamirim (72%) e Caicó (67%). Os autores ainda concluíram que os municípios pesquisados precisam melhorar o nível de transparência de suas informações, para que os cidadãos possam ter um melhor contato com o que é disponibilizado em seus portais eletrônicos, e para que a população possa exercer o controle social mais eficaz perante as ações dos atos da gestão pública.

Herculano e Chiarello (2015) investigaram o impacto da assimetria de informação na relação entre participação e folga orçamentária, especialmente no cenário da gestão de universidades públicas, com vistas a minimizar os conflitos sobre a eficácia do planejamento, as razões do uso do orçamento e a participação no orçamento. Os resultados obtidos indicaram que o uso do orçamento na instituição pública está concentrado na reitoria e coordenadoria de gestão, o que demonstrou alta assimetria da informação entre os servidores e a gestão. Além disso, os autores observaram que há relação entre a participação dos subordinados no orçamento e folga orçamentária. Por fim, os autores observaram ainda que não existe relação estatística entre a assimetria de informação tanto com a participação como na folga orçamentária.

Corrêa da Silva e Gomes da Silva (2015) avaliaram a execução orçamentária dos 50 municípios mais populosos do Brasil por funções de governo, no ano de 2013, utilizando a técnica da Análise de Componentes Principais (ACP), a fim de elaborar um índice e estabelecer um *ranking* de desempenho. Os dados sobre as funções de governo foram extraídos do sítio eletrônico da Secretaria do Tesouro Nacional (STN). Os resultados evidenciaram que os municípios de Campos dos Goytacazes (RJ), Belo Horizonte (MG) e Caxias do Sul (RS) obtiveram os melhores desempenhos da execução orçamentária por funções de governo no ano de 2013. Os municípios de Maceió (AL), São Gonçalo (RJ) e Nova Iguaçu (RJ) apresentaram os piores desempenhos.

Por último, Santos et al. (2017) analisaram o papel da técnica orçamento-programa na execução de políticas públicas no Estado brasileiro. Os autores constataram que o orçamento público baseado em programas é um importante instrumento multidimensional de gestão e de implementação de políticas públicas. Também concluíram que as organizações da sociedade civil, os atores sociais e os grupos de interesse têm no orçamento-programa um importante

instrumento de controle para cobrar da administração pública uma maior eficácia nos gastos destinados aos programas de políticas públicas.

Ante o exposto acima, é possível então principalmente constatar que há: baixo nível de transparência, deficiências na divulgação obrigatória, baixa aderência às práticas de evidenciação voluntária, impossibilidade de exercício de controle mais eficaz; alta assimetria da informação entre os servidores envolvidos e a própria gestão. Ainda, é possivel afirmar que um orçamento público baseado em programas é um importante instrumento de gestão e de implementação de políticas públicas. Esse cenário motiva a proposição de soluções que vislumbrem a automatização do modelo de gestão, que é exatamente o objetivo precípuo deste trabalho.

3. Sistema de Pagamento Eletrônico *Bitcoin*

O protocolo *Bitcoin* foi originalmente anunciado em um artigo publicado em novembro do ano de 2008, o qual definiu uma forma de criptomoeda que funciona de forma pseudônima e sem depender da confiança de qualquer usuário do sistema (NAKAMOTO, 2008). Esse protocolo foi desenvolvido considerando o paradigma de uma rede *peer-to-peer* (*P2P*) de alcance mundial, resultando em um sistema de pagamento eletrônico de transações financeiras de escala global (SILVA e RODRIGUES, 2016; RODRIGUES, 2017).

A operação do sistema é essencialmente baseada na gerência eficiente de um *ledger* público (livro-razão), baseado em *blockchain*. Esse *ledger* contém todas as transações realizadas desde a criação do sistema, permitindo a todos os participantes verificarem o histórico de cada transação. A autenticidade de cada transação é protegida por assinaturas digitais, associadas aos endereços *bitcoin* de quem as realizou.

Qualquer participante do sistema pode realizar a validação de transações e ganhar uma recompensa por esse serviço. Essa tarefa é chamada de mineração, e aquele que a realiza é chamado de minerador. Toda vez que uma transação é realizada e verificada, o *ledger* público é atualizado em todos os nós do sistema (ROTH, 2015; FELD et al., 2014).

Quando o pagador de uma transação em *bitcoins* envia certa quantia para outro usuário do sistema é como se esse pagador estivesse assinando um documento público que atesta a transferência de posse daquela quantia para aquele outro usuário. A assinatura dessa transação é realizada pelo conceito de par de chaves assimétricas (KUROSE e ROSS, 2013), onde um mesmo usuário da rede possui duas sequências de dígitos únicos que formam as chaves pública e privada, respectivamente.

O sistema de chaves criptográficas assimétricas garante a autenticidade de quem e para quem a transação é realizada, mas não garante que um mesmo usuário não possa gastar aquela mesma quantia mais de uma vez em outras transações. Dado que se decorre um tempo para propagar-se o *ledger* atualizado, qualquer usuário poderia teoricamente realizar outra transação enquanto a antiga não tivesse se propagado por toda a rede. Nesse caso, a rede teria dificuldades em diferenciar qual transação seria a legítima. Esse problema é denominado de gasto em duplicidade, sendo resolvido pelo uso do conceito de *blockchain*, conforme explicado nos passos a seguir (NIELSEN, 2013).

1) Propagam-se por toda a rede as transações recém realizadas, mas ainda não validadas. Essas transações são então agrupadas em blocos. Cada bloco é validado pelos mineradores no processo de mineração;

2) Após validado, o bloco é então adicionado a uma cadeia de blocos, que leva desde o primeiro bloco, contendo a primeira transação já realizada na história do sistema *Bitcoin*, até a transação mais recentemente validada;

3) Os blocos que não forem validados pelos mineradores são descartados. Essa corrente é denominada de *blockchain* e é a base de informação para implementar o *ledger* público.

Nakamoto (2008) definiu que o processo matemático realizado pelo minerador ocorre por meio do algoritmo *hash* criptográfico SHA-256. Esse algoritmo faz com que minerador precise descobrir um número inteiro de 4 bytes, denominado de *nonce*, capaz de satisfazer a uma desigualdade matemática expressa em função desse algoritmo.

O método de descobrimento usado pelo minerador é baseado em múltiplas tentativas, e a condição de desigualdade é estabelecida considerando-se um valor máximo, denominado de *target difficulty*, que é ajustado pelo algoritmo para garantir que, em média, apenas um bloco de transações válidas seja adicionado à *blockchain* a cada 10 minutos.

O *nonce* descoberto, também chamado de *golden nonce*, é a *proof-of-work* (i.e., prova de trabalho) que o cálculo iterativo por tentativas foi de fato realizado e que o bloco pode então ser adicionado à *blockchain* (ROCHA e RODRIGUES, 2016). Para incentivar os mineradores a validar os blocos, o protocolo prevê uma recompensa em *bitcoins* para quem primeiro conseguir encontrar o *golden nonce*. Essa recompensa não tem um valor fixo, sendo alterada de tempos em tempos (ROSENFELD, 2016).

Quando o sistema *Bitcoin* foi lançado, a recompensa era de 50,0 *bitcoins*. Esse valor de recompensa é dividido por 2 a cada 230.000 blocos minerados na rede ou, aproximadamente, a cada quatro anos, já que cada bloco leva cerca de dez minutos para ser minerado. Esse ajuste é conhecido como *halving*. O sistema *Bitcoin* já passou por dois *halvings* e, atualmente, cada bloco minerado é recompensado com 12,5 *bitcoins*.

Destaca-se a importância do trabalho de Rocha e Rodrigues (2016), o qual apresenta a modelagem do processo de negócio do sistema *Bitcoin* usando técnicas de Engenharia de *Software* e de *Business Process Model and Notation* (BPMN). Os modelos desenvolvidos facilitam o entendimento funcional do sistema como um todo e de suas partes individuais constituintes. Sob esse mesmo viés, Roth (2015) emprega a linguagem SysML (*Systems Modeling Language*) para esclarecer a estrutura da arquitetura do sistema. Esses dois trabalhos são indicados para os leitores que desejam um maior detalhamento da arquitetura do sistema *Bitcoin*.

4. Automatização da Gestão Financeira e Orçamentária Baseada em *Blockhain* e *Bitcoin*

4.1. Entendendo o Problema

Sob o modelo da gestão pública brasileira, a Figura 1 mostra um fluxograma elementar das principais atividades a serem desencadeadas sequencialmente para se obter um produto a partir de um fornecedor. Esse fluxograma se respalda em conceitos da disciplina de Execução Orçamentária e Financeira (FEIJÓ et al., 2014; FEIJÓ e RIBEIRO, 2014; BRASIL, 2015).

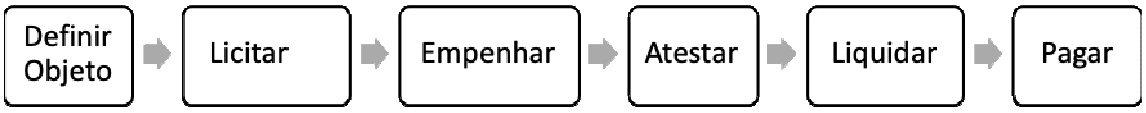

Figura 1. Fluxograma simplificado de obtenção de produto ou serviço

Os entendimentos básicos das atividades do fluxograma da Figura 1 são dados a seguir (FEIJÓ et al., 2014; BRASIL, 2015). *Definir Objeto* consiste em identificar precisamente o produto que se deseja obter, explicitando todas as suas caraterísticas de modo a não deixar quaisquer questões em aberto que venham a permitir dubiedades de entendimento. *Licitar* consiste em tornar público o objeto pretendido de tal maneira que distintas empresas possam livremente disputar o direito de poder fornecer o objeto.

Empenhar se refere ao ato de formalizar que a empresa vencedora da licitação passa a ter o direito de receber o valor financeiro do objeto a ser entregue. *Atestar* diz respeito à atividade de verificar se o produto entregue pela empresa vencedora está em conformidade com o desejado. *Liquidar* é ato formal que informa que o valor do produto pode ser pago à empresa que o entregou. Por último, *Pagar* é o ato de realizar uma transferência bancária no valor do produto para a empresa.

Em complemento, a Figura 2 representa de forma simplificada o ciclo integrado do modelo de planejamento e orçamento do sistema público brasileiro (FEIJÓ et al., 2014; BRASIL, 2015; ALBUQUERQUE et al., 2013). São três instrumentos básicos: o Plano Plurianual (PPA), a Lei de Diretrizes Orçamentárias (LDO) e a Lei Orçamentária Anual (LOA). O PPA, com vigência de quatro anos, estabelece diretrizes, objetivos e metas de médio prazo da administração pública. A LDO anualmente enuncia as políticas públicas e as respectivas prioridades para o exercício do ano seguinte. Já a LOA principalmente estima a receita e fixa a programação das despesas para o exercício financeiro corrente (BRASIL, 2015).

A LDO, portanto, ao identificar no PPA as ações que vão receber prioridade no exercício do ano seguinte, acaba por ser o elo entre o PPA, que constitui um plano de médio-prazo do governo, e a LOA, que viabiliza a execução do plano de trabalho do exercício a que se refere. Em acordo com a Constituição Federal, a função do planejamento é um dever do Estado, possuindo caráter determinante para o setor público e indicativo para o setor privado (BRASIL, 2015).

As fases Execução Orçamentária e Financeira e Controle e Avaliação finalizam o ciclo da Figura 2 e se referem, como as próprias denominações sugerem, a execução do que foi planejado nas fases anteriores e o corresponde exercício de controle e avaliação, respectivamente.

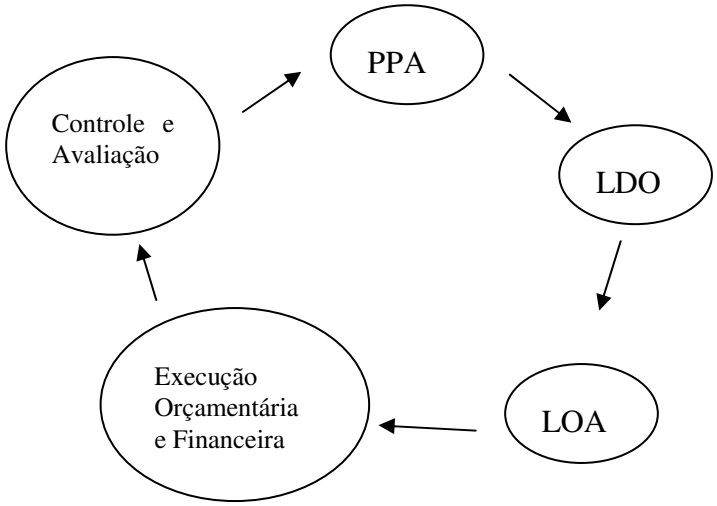

Figura 2. Ciclo integrado do modelo de planejamento e orçamento

As Figuras 1 e 2 retratam conjuntamente o cenário complexo que deve ser enfrentado ao planejar-se a aquisição de um produto dentro de um planejamento macro de gestão. Em específico, a Figura 1 explicita as ações a serem desencadeadas para cada aquisição que venha a existir. No entanto, é preciso perceber a relação dessa aquisição com o planejamento macro da gestão pública orçamentária e financeira do país, descrito na Figura 2. Para que o planejamento macro (Figura 2) seja bem-sucedido é importante que cada aquisição (Figura 1) seja bem-sucedida. Há uma interdependência natural.

Esse cenário complexo possui variáveis, indicadores e metas das mais diversas naturezas, que são intrincadas de serem perfeitamente identificadas e quantificadas, tendo-se especial atenção à classificação das despesas por meio do sistema de códigos numéricos, comentado no início deste trabalho (FEIJÓ et al., 2014). Na prática, exigem-se, por ofício, frequentes alterações e/ou adaptações ao longo do tempo que esbarram na inflexibilidade daquilo que formalmente, sob pena da lei, deve ser previamente definido.

Além disso, outra questão imperiosa é que o controle e a avaliação da execução são difíceis de serem adequadamente implementados em face do nível de detalhamento previsto e da falta de automatização dos processos. Há óbices claros que, muitas das vezes, são muito dificilmente transponíveis.

4.2. Proposta de Automatização

O complexo cenário descrito na subseção anterior pode ser eficientemente tratado a partir da automatização dos processos das Figuras 1 e 2, respectivamente, conforme discorrido a seguir.

Partindo-se da Figura 2, por ser o processo maior e que representa em primeira instância o interesse macro da nação, observa-se o seguinte. PPA, LDO e LOA constituem-se em fases caracterizadas precipuamente por aspectos político, econômico e estratégico. São tomadas decisões para alocação de recursos que, incialmente, são orçamentários e que, em seguida, são utilizados para execução financeira.

Uma vez que as decisões tenham sido tomadas, a eventual automatização dessas fases do ciclo da Figura 2 traz como aspecto inovador a obrigatoriedade de execução do que foi originalmente planejado, sob pena de retorno dos recursos à origem da fonte pagadora, ou, alternativamente, a inteira transparência dos eventuais ajustes ou modificações com relação ao originalmente planejado.

Isso é conseguido por meio da implementação dos chamados *smart contracts* (contratos inteligentes), os quais são programados em linguagem computacional para terem seus eventos executados quando as condições exigidas são atendidas. Alguns tipos de contratos inteligentes são programados em plataformas baseadas em criptomoedas (neste caso em *bitcoins*)[2]. Essa programação permite inclusive alterar o significado do *bitcoin* dentro da *blockchain*. Para implementação da *blockchain*, não importa se 1,0 *bitcoin* representa um montante de reais ou de dólares, ou de qualquer outra referência de valor ou de propriedade.

Por definição, 1,0 *bitcoin* é divisível em 100 milhões de unidades e cada unidade é individualmente identificável e programável (NAKAMOTO, 2008). Isso pois significa que os clientes do sistema podem atribuir propriedades para cada unidade. É na realidade um processo de contagem e controle de recursos, não importando a natureza constitutiva dos mesmos.

Ainda na Figura 2, têm-se as fases Execução Orçamentária e Financeira e Controle e Avaliação. Essas duas últimas fases se referem a observar para que aquilo que foi acordado nas fases anteriores seja perfeitamente cumprido ou, se necessário, corretamente ajustado. Uma vez que tenha ocorrido a automatização, essa tarefa de observação ou eventual ajuste se torna de simples execução, pois implica apenas, quando necessário, em alteração de regras (escritas em linguagem de programação) dos *smart contracts*.

Essas duas últimas fases do ciclo da Figura 2 também se relacionam com as aquisições de produtos que vierem a ser realizadas por meio do desencadeamento do processo da Figura 1. Por exemplo, quando se destina um recurso de *X* milhões de reais para o Ministério da Saúde (resultante da alocação de recursos definida no ciclo da Figura 2), o que se deseja é que todos os gestores envolvidos com aquele Ministério realizem contratações responsáveis de aquisições de produtos (conforme estabelecido no processo da Figura 1) que estejam de acordo com o montante estabelecido de *X* milhões de reais. Por contratações responsáveis, entendam-se aquelas que observam o correto uso do dinheiro público.

Veja então que o processo da Figura 1 pode se repetir centenas de vezes para que o montante de *X* milhões de reais seja devidamente empregado. A automatização vislumbrada aqui consiste também na implementação de *smart contracts* para todas as aquisições que vierem a se realizar em todas as entidades públicas. Mais especificamente, *smart contracts* automatizariam desde a fase *Empenhar* até a fase *Pagar* do processo da Figura 1.

A automatização descrita acima pode levar a uma significativa diminuição de burocracia, reduzindo a necessidade de contadores, supervisores, controladores e auditores, bem como otimizando o tempo de execução dos processos administrativos em geral. É possível, assim, imaginar a reconstrução e a inovação dos setores orçamentários e financeiros e, também, de todos os processos administrativos associados, estabelecendo um paradigma bem mais eficiente e eficaz.

Dentre os principais benefícios, a automatização proposta permitiria: maior nível de transparência, pois os *smart contracts* podem ser divulgados publicamente; divulgação facilitada de relatórios de gestão, pois os *smart contracts* podem implementar a distribuição de relatórios periódicos para todos os atores envolvidos; exercício de controle mais eficaz, pois os *smart contracts* somente são alterados de forma transparente; maior simetria da

[2] Originalmente os Smart Contracts (Contratos Inteligentes) foram baseados em *Bitcoin*, com a evolução, passaram a ser independente de cripotomoedas, um exemplo é o hyperledger fabric (HYPERLEDGER, 2018).

informação entre os servidores envolvidos e a própria Gestão, pois os *smart contracts* permitem a elaboração conjunta das regras e de eventuais ajustes de maneira transparente. Indubitavelmente, passa a existir um efetivo instrumento de controle para cobrar da administração pública uma maior efetividade nos gastos destinados aos programas de políticas públicas.

Essa discussão teórica se aplica semelhantemente aos setores da economia privada e vale também para qualquer país no mundo que necessite de automatização de gestão orçamentária e financeira. Diante disso, surge então a seguinte questão: como realizar *smart contracts* baseados em *bitcoins*? A resposta para essa questão é dada na seção seguinte, onde sucintamente se descreve a plataforma *Ethereum* (WOOD, 2015), a qual nasceu com a intenção de prover um ambiente adequado para implementação de *smart contracts* baseados em criptomoedas.

4.3. Ambiente *Ethereum*

Ethereum constitui um ambiente para implementação da plataforma de Gestão da Execução e Controle Orçamentário baseada em *smart contracts* e criptomoedas, proposta na seção anterior. Esse ambiente flexibiliza a definição semântica do conteúdo a ser guardado na base de dados, i.e., na *blockchain*. Isso com o intuito de prover uma plataforma geral de *smart contracts* sem a dependência de terceiras partes confiáveis para validação e controle das transações realizadas.

Ethereum é, sob o viés computacional, uma pilha de protocolos implementando uma plataforma para a execução de aplicações descentralizadas de qualquer complexidade em máquinas virtuais. Essas aplicações são criadas usando linguagens de programação já existentes, como JavaScript e Python. A *blockchain* do *Ethereum* é mantida e atualizada por inúmeros nós conectados entre si, formando uma rede P2P de escala mundial (ETHEREUM HOMESTEAD, 2016).

A paralelização provida pelos nós da rede *Ethereum* não objetiva a eficiência computacional, mas sim a garantia de um consenso entre seus nós para manter a consistência dos dados da *blockchain*. O consenso descentralizado garante um alto nível de tolerância a falhas, assegura a continuidade de serviço, e torna a *blockchain* praticamente impossível de ser fraudada (WOOD, 2015).

Ethereum é espontaneamente aderente àquelas aplicações que visualizam automatizar a interação direta entre pares ou facilitar a interação de grupos na rede. Por exemplo, aplicações que envolvem coordenação de mercados financeiros ou a automatização de contratos financeiros de transações estabelecidas por regras complexas. No entanto, além da gestão orçamentária e financeira, esse ambiente se aplica a quaisquer aplicações que exijam confiança, segurança, não volatilidade e continuidade de serviço como, por exemplo, registros de ativos, sistemas de votação, governança e na implementação do conceito de *Internet of things* (FARRIS et al., 2017).

A unidade básica do *Ethereum* é a conta. A *blockchain* registra os estados de cada conta, e todas as transições de estado são transferências de valores e de informações entre contas. Há dois tipos de contas: contas externas proprietárias (EOAs - *Externally Owned Accounts*), que são controladas por chaves privadas, e contas contratos (CAs - *Contract Accounts*), que são controladas por código computacional e ativadas apenas por uma conta externa proprietária.

Pessoas físicas controlam as contas externas proprietárias, enquanto que as contas contratos são controladas pelas regras implementadas por meio de codificação em linguagem de programação. O termo *smart contract* se refere ao código contido em uma conta contrato. Novos contratos são criados quando códigos são acrescidos à *blockchain*. As operações das contas contratos ocorrem apenas quando solicitadas por uma conta externa proprietária.

Os clientes do ambiente *Ethereum* devem pagar uma taxa por transação realizada. Isso protege a *blockchain* de atividades frívolas ou mal-intencionados, como ataques de DDoS ou *loops* infinitos (KUROSE e ROSS, 2013). O emissor de uma transação deve pagar por cada etapa do programa que é ativado, incluindo a computação realizada e o armazenamento em memória. Essas taxas são pagas em quantidades de valor virtual (i.e., criptomoeda) denominado de *ether*. A criptomoeda *ether* tem a mesma concepção conceitual da criptomoeda *bitcoin* e, portanto, permite a discussão que aqui se realiza.

Semelhantemente ao já discutido anteriormente, as taxas de transação são recebidas pelos nós que validam a rede, os chamados mineradores. Eles recebem, propagam, verificam, executam e também agrupam as transações, incluindo as atualizações de estado das contas, em blocos. Um minerador é recompensado com um montante em *ether* quando seu bloco é o primeiro a ser minerado na rede, significando que a *proof-of-work* foi realizada por ele. Também como antes, a recompensa visa a prover um incentivo econômico para que os mineradores invistam seu poder computacional de *hardware* em prol do ambiente *Ethereum*.

É importante destacar que a *proof-of-work* do ambiente *Ethereum* é escolhida de modo a desencorajar o uso de *hardware* especializado como ASICs (*Application Specific Integrated Circuits*). Para isso, o problema a ser resolvido como *proof-of-work* é baseado em uso intensivo de memória. Como consequência, dado que a solução desse problema requer tanto memória como *hardware*, o hardware ideal passa a ser um computador de uso geral, resultando em uma providencial descentralização da segurança do ambiente *Ethereum*.

5. Conclusões e Trabalhos Futuros

Este artigo teve por objetivo propor o emprego do sistema de pagamento eletrônico *Bitcoin* para automatizar a gestão pública orçamentária e financeira do Brasil.

Para alcançar-se este objetivo, inicialmente apresentou-se uma visão geral do sistema *Bitcoin*. Logo depois, comentou-se sobre o modelo vigente de gestão orçamentária e financeira pública do Brasil. Na sequência, realizou-se uma discussão sobre o que automatizar nesse modelo e as vantagens decorrentes. Finalmente, fez-se uma breve explicação do ambiente computacional *Ethereum* (WOOD, 2015), onde a automatização proposta pode ser implementada na prática.

A partir das discussões aqui apresentadas e baseando-se também em resultados de trabalhos anteriores da literatura, foi possível concluir favoravelmente sobre a robustez tecnológica para a área financeira desse ambiente de computação distribuída baseado em *Bitcoin*, bem como vislumbrar a diminuição significativa da burocracia e aumento da eficácia do modelo de gestão pública orçamentária e financeira do Brasil.

Dentre outros importantes benefícios, a automatização aqui proposta permitiria: maior nível de transparência; divulgação facilitada de relatórios de gestão; exercício de controle mais eficaz; maior simetria da informação entre os servidores envolvidos e a própria gestão. Em síntese, passa-se a existir um importante instrumento de controle para cobrar da

administração pública uma maior efetividade nos gastos destinados aos programas de políticas públicas.

O uso de tecnologia da informação para aumentar a eficiência da gestão pública e do controle orçamentário já é adotado em diversos países. No Brasil, a Secretária do Tesouro Nacional (STN) adotou no projeto SICONFI (Sistema de Informações Contábeis e Fiscais) o padrão internacional para a representação e intercâmbio de dados financeiros, denominado XRBL (*eXtensible Business Reporting Language*). A proposta apresentada neste artigo, aliada à utilização de um padrão para intercâmbio de dados, já utilizado pela STN, possibilitaria uma melhor eficiência na gestão pública, além de facilitar a integração dos entes públicos (municípios, estados e órgão federais) com o Tesouro Nacional, aumentando a transparência e proporcionando melhor controle sobre os gestores públicos a respeito do atendimento da Lei de Responsabilidade Fiscal. O estudo do ambiente proposto, tendo como modelo de dados baseado em XBRL, é um trabalho a ser efetuado, de forma que seja possível uma melhor integração desse ambiente com o SICONFI.

Como trabalhos futuros, recomendam-se os seguintes dois estudos de caso (HEVNER, 2004). Primeiro, a análise do emprego do ambiente *Ethereum* para automatização da gestão orçamentária e financeira de um pequeno município do Brasil, mas mantendo-se em simultâneo o modelo tradicional. Isso permitiria ratificar, por meio de simples comparação, a expectativa de redução da burocracia existente, bem como da efetividade do novo modelo automatizado. Em se comprovando a expectativa de resultados positivos, seguir-se-ia então para a automatização da gestão orçamentária e financeira dos Estados e, por fim, de todo o país. Segundo, o estudo é a análise da viabilidade de emprego do ambiente *Ethereum* para a gestão orçamentária e financeira do setor privado do Brasil, considerando empresas de pequeno, médio e grande porte, mas também se mantendo em simultâneo o modelo tradicional de gestão. Como antes, isso permitiria, por simples comparação, ratificar a expectativa de redução da burocracia existente, bem como da efetividade do novo modelo automatizado.

Referências

ALBUQUERQUE, C. M.; MEDEIROS, M. B.; FEIJÓ, P. H. Gestão de Finanças Públicas: Fundamentos e Práticas de Planejamento, Orçamento e Administração Financeira com Responsabilidade Fiscal. Volume I – Administração Financeira e Orçamentária. 3ª ed. Brasília: Gestão Pública, 2013.

BAIRRAL, M. A. C.; COUTINHO E SILVA, A. H.; ALVES, F. J. S. Transparência no setor público: uma análise dos relatórios de gestão anuais de entidades públicas federais no ano de 2010. Revista de Administração Pública, v. 49, n. 3, p. 643-675, 2015.

BRASIL. Ministério do Planejamento, Orçamento e Gestão. Secretaria de Orçamento Federal. Manual técnico de orçamento MTO. 2015. Edição 2016. Brasília, DF.

CORRÊA DA SILVA, M.; GOMES DA SILVA, J. D. Ranking de desempenho da execução orçamentária por funções de governo dos 50 municípios mais populosos do brasil em 2013 e determinação de suas funções significativas. InterSciencePlace - Revista Científica Internacional, v. 10, n. 3, artigo 8, julho/setembro, 2015.

DE SOUZA, F. J. V.; BARROS, C. C.; ARAÚJO, F. R.; DA SILVA, M. C. Índice de transparência municipal: um estudo nos municípios mais populosos do Rio Grande do Norte. Revista de Gestão, Finanças e Contabilidade, v. 3, n. 3, p. 94-113, 2003.

DYHRBERG, A. H. Bitcoin, gold and the dollar – a GARCH volatility analysis. Finance Research Letters, v. 16, p. 85-92, February, 2016.

ETHEREUM HOMESTEAD. Ethereum Homestead Documentation. Disponível em: http://www.ethdocs.org/en/latest/. Acesso em: jul. 2016.

FARRIS, I.; Leonardo MILITANO, L.; NITTI, M.; ATZORI, L.; LERA, A. MIFaaS: A Mobile-IoT-Federation-as-a-Service Model for dynamic cooperation of IoT Cloud Providers. Future Generation Computer Systems, v. 70, p. 126-137, 2017.

FEIJÓ, P. H.; PINTO, L. F.; MOTA, F. G.; DA SILVA, L. C. Curso de SIAFI: Uma abordagem prática da execução orçamentária financeira. 3a. ed., Volume I, Brasília: Gestão Pública. 2014.

FEIJÓ, P. H.; RIBEIRO, C. E. Entendendo o Plano de Contas Aplicado ao Setor Público: PCASP – Exercícios e Estudo de Caso com Lançamentos Típicos. Série Entendendo CASP. 1ª ed., Brasília: Gestão Pública. 2014.

FELD, S.; SCHÖNFELD, M.; MARTIN, W. Analyzing the deployment of Bitcoin's P2P network under an AS-level perspective. Procedia Computer Science, v. 32, p.1121–1126, 2014.

HENDERSON, L. S. Encoding and decoding communication competencies in project management: an exploratory study. International Journal of Project Management, v. 22, p. 469-476, 2004.

HERCULANO, H. A.; CHIARELLO, T. C. Assimetria de Informação na Relação entre Participação e Folga Orçamentária. In: 1º Congresso UnB de Contabilidade e Governança. O papel da contabilidade na governança das instituições públicas e privadas, Brasília, 26 a 27 de novembro de 2015. Anais…Brasília, 2015.

HEVNER, A. R.; MARCH, S. T.; PARK, J.; RAMET, S. Design Science in Information Systems Research. MIS Quarterly, v. 28, n. 1, p. 75-105, 2004. Disponível em: https://doi.org/10.2307/25148625. Acesso em: dez. 2018.

HYPERLEDGER Fabric Project. Disponível em: https://www.hyperledger.org/projects/fabric. Acesso em: dez. 2018

IKA, L. A. Project success as a topic in project management journals. Project Management Journal, v. 40, n. 4, p. 6-19, 2009.

KUROSE, J. F.; ROSS, K. W. Computer networking: A top-down approach featuring the Internet. 6th ed. New York: Pearson Education, 2013.

LANTMÄTERIET; LANDSHYPOTEK Bank; SBAB; TELIA company; CHROMAWAY and KAIROS Future. The Land Registry in the blockchain March 2017. Disponível em: https://chromaway.com/papers/Blockchain_Landregistry_Report_2017.pdf. Acesso em: dez. 2018.

LUTHER, W. J. Bitcoin and the Future of Digital Payments. 2015. Disponível em: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2631314. Acesso em: fev. 2016.

NAKAMOTO, S. Bitcoin: A Peer–to–peer Electronic Cash System. 2008. Disponível em: http://www.bitcoin.org/bitcoin.pdf. Acesso em: jul. 2015.

NIELSEN, M. How the Bitcoin protocol actually works. 2013. Disponível em: http://www.michaelnielsen.org/ddi/how-the-bitcoin-protocol-actually-works/. Acesso em: fev. 2016.

ROCHA, J. G.; RODRIGUES, C. K. S. O Processo de Negócio do Sistema de Transações Financeiras Bitcoin. Universitas: Gestão e TI, v. 6, n. 1, p. 1-10, julho, 2016.

RODRIGUES, C. K. S. Sistema Bitcoin: uma análise da segurança das transações. iSys | Revista Brasileira de Sistemas de Informação, v. 10, n. 3, pp. 5-23, 2017

ROSENFELD, M. Analysis of Bitcoin Pooled Mining Reward Systems. 2011. Disponível em: http://arxiv.org/pdf/1112.4980v1.pdf. Acesso em: jul. 2016.

ROTH, N. An architectural assessment of Bitcoin: using the System Modeling Language. Procedia Computer Science, v. 44, p. 527-536, 2015.

SILVA, G. A.; RODRIGUES, C. K. S. Mineração individual de bitcoins e litecoins no mundo. In: Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg 2016), Niterói, Rio de Janeiro, Brasil, 2016.